Junos® OS

User Access and Authentication Feature Guide

Published 2019-10-22
Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

**Junos**® **OS User Access and Authentication Feature Guide**  
Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

**YEAR 2000 NOTICE**

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

**END USER LICENSE AGREEMENT**

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at [https://support.juniper.net/support/eula/](https://support.juniper.net/support/eula/). By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
Passwords for User Access

Root Password | 177
- Configuring the Root Password | 177
- Example: Configuring a Plain-Text Password for Root Logins | 179
- Example: Configuring SSH Authentication for Root Logins | 182

Recovering Root Password | 183
- Recovering the Root Password | 183
- Recovering the Root Password on Junos OS with Upgraded FreeBSD | 186
- Recovering the Root Password for Junos OS Evolved | 189
  - Connecting to the Serial Port | 189
  - Recovering the Root Password | 191
- Troubleshooting Loss of the Root Password | 193

Plain-Text Passwords | 196
- Changing the Requirements for Junos OS Plain-Text Passwords | 196
- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

Master Password for Configuration Encryption | 200
- Hardening Shared Secrets in Junos OS | 200
  - Understanding Hardening Shared Secrets | 200
- Using Trusted Platform Module to Bind Secrets on SRX Series Devices | 202
  - Limitations | 203
  - Enabling the TPM | 204
  - Verifying the Status of the TPM | 204
  - Changing the Master Encryption Password | 204
User Authentication

Junos OS User Authentication Overview | 209
- Junos OS User Authentication Methods | 209
- Configuring Local User Template Accounts for User Authentication | 210
- Configuring Remote Template Accounts for User Authentication | 212
- Example: Creating Template Accounts | 213
- Understanding Remote Authentication Servers | 217

Authentication Order for RADIUS, TACACS+, and Local Password | 218
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication | 218
  - Using RADIUS or TACACS+ Authentication | 219
  - Using Local Password Authentication | 220
  - Order of Authentication Attempts | 220
- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication | 225
  - Example: Configuring Authentication Order | 227
  - Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication | 230

RADIUS Authentication | 233
- Configuring RADIUS Server Authentication | 233
  - Why Use RADIUS | 234
  - Configuring RADIUS Server Details | 234
  - Configuring RADIUS To Use the Management Instance | 238
  - Example: Configuring a RADIUS Server for System Authentication | 239
  - Example: Configuring RADIUS Authentication | 243
- Configuring RADIUS Authentication (QFX Series or OCX Series) | 244
  - Configuring RADIUS Server Details | 245
  - Configuring MS-CHAPv2 for Password-Change Support | 246
  - Specifying a Source Address for the Junos OS to Access External RADIUS Servers | 247
  - Juniper Networks Vendor-Specific RADIUS Attributes | 247
  - Juniper- Switching-Filter VSA Match Conditions and Actions | 251
- Understanding RADIUS Accounting | 254
Configuring Outbound SSH Clients | 310
Configuring Routing Instances for Outbound SSH Clients | 310
Configuring NETCONF-Over-SSH Connections on a Specified TCP Port | 310
Configuring Password Retry Limits for Telnet and SSH Access | 311
Example: Configuring a Filter to Block Telnet and SSH Access | 312

USB Modems for Remote Management of Security Devices | 319
USB Modem Interface Overview | 320
USB Modem Interfaces | 321
Dialer Interface Rules | 321
How the Device Initializes USB Modems | 322
USB Modem Configuration Overview | 323
Example: Configuring a USB Modem Interface | 326
Example: Configuring a Dialer Interface | 329
Example: Configuring a Dialer Interface for USB Modem Dial-In | 334
Configuring a Dial-Up Modem Connection Remotely | 336
Connecting to the Device Remotely | 337
Modifying USB Modem Initialization Commands | 337
Resetting USB Modems | 338

Secure Web Access for Remote Management | 339
Secure Web Access Overview | 340
Generating SSL Certificates for Secure Web Access (SRX Series Devices) | 340
Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch) | 341
Generating a Self-Signed SSL Certificate Automatically | 342
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually Generating Self-Signed SSL Certificates</td>
<td>342</td>
</tr>
<tr>
<td>Deleting Self-Signed Certificates (CLI Procedure)</td>
<td>343</td>
</tr>
<tr>
<td>Understanding Self-Signed Certificates on EX Series Switches</td>
<td>344</td>
</tr>
<tr>
<td>Manually Generating Self-Signed Certificates on Switches (CLI Procedure)</td>
<td>345</td>
</tr>
<tr>
<td>Generating a Public-Private Key Pair on Switches</td>
<td>345</td>
</tr>
<tr>
<td>Generating Self-Signed Certificates on Switches</td>
<td>346</td>
</tr>
<tr>
<td>Example: Configuring Secure Web Access</td>
<td>346</td>
</tr>
<tr>
<td>Example: Controlling Management Access on SRX Series Devices</td>
<td>349</td>
</tr>
<tr>
<td>Configuration Guidelines for Securing Console Port Access</td>
<td>354</td>
</tr>
<tr>
<td>Securing Console Port</td>
<td>354</td>
</tr>
<tr>
<td>Securing Mini-USB Ports</td>
<td>356</td>
</tr>
<tr>
<td>Access Control on Switches</td>
<td>361</td>
</tr>
<tr>
<td>Access Control and Authentication on Switching Devices</td>
<td>361</td>
</tr>
<tr>
<td>Understanding Authentication on Switches</td>
<td>361</td>
</tr>
<tr>
<td>Sample Authentication Topology</td>
<td>362</td>
</tr>
<tr>
<td>802.1X Authentication</td>
<td>364</td>
</tr>
<tr>
<td>MAC RADIUS Authentication</td>
<td>365</td>
</tr>
<tr>
<td>Captive Portal Authentication</td>
<td>366</td>
</tr>
<tr>
<td>Static MAC Bypass of Authentication</td>
<td>366</td>
</tr>
<tr>
<td>Fallback of Authentication Methods</td>
<td>367</td>
</tr>
<tr>
<td>Understanding Access Control on Switches</td>
<td>368</td>
</tr>
<tr>
<td>Understanding Authentication Session Timeout</td>
<td>370</td>
</tr>
<tr>
<td>Controlling Authentication Session Timeouts (CLI Procedure)</td>
<td>371</td>
</tr>
<tr>
<td>Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot</td>
<td>373</td>
</tr>
<tr>
<td>Understanding Unattended Mode for U-Boot on EX Series Switches</td>
<td>373</td>
</tr>
<tr>
<td>Using Unattended Mode for U-Boot to Prevent Unauthorized Access</td>
<td>375</td>
</tr>
<tr>
<td>Configuring the Boot Loader Password</td>
<td>376</td>
</tr>
<tr>
<td>Configuring Unattended Mode for U-Boot</td>
<td>377</td>
</tr>
<tr>
<td>Accessing the U-Boot CLI</td>
<td>377</td>
</tr>
</tbody>
</table>
RADIUS Server Configuration for Authentication | 378
Specifying RADIUS Server Connections on Switches (CLI Procedure) | 379
Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure) | 380
Configuring MS-CHAPv2 for Password-Change Support | 381
Understanding Server Fail Fallback and Authentication on Switches | 383
Configuring RADIUS Server Fail Fallback (CLI Procedure) | 384

802.1X Authentication | 386
802.1X for Switches Overview | 387
How 802.1X Authentication Works | 387
802.1X Features Overview | 388
802.1X Authentication on Trunk Ports | 389
Configuring 802.1X Interface Settings (CLI Procedure) | 390
Understanding RADIUS-Initiated Changes to an Authorized User Session | 392
Disconnect Messages | 392
Change of Authorization Messages | 393
CoA Request Port Bounce | 393
Error-Cause Codes | 394
Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395
Configuring Firewall Filters on the RADIUS Server | 396
Applying a Locally Configured Firewall Filter from the RADIUS Server | 399
Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
Understanding Dynamic Filters Based on RADIUS Attributes | 405
Understanding Dynamic VLAN Assignment Using RADIUS Attributes | 406
Understanding Guest VLANs for 802.1X on Switches | 407
Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 408
Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients | 415
Monitoring 802.1X Authentication | 420
Verifying 802.1X Authentication | 421
Troubleshooting Authentication of End Devices on EX Series Switches | 423

MAC RADIUS Authentication | 425
Configuring MAC RADIUS Authentication (CLI Procedure) | 426
Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 427
802.1X and RADIUS Accounting | 434

Understanding 802.1X and RADIUS Accounting on Switches | 435
RADIUS Accounting Process | 435
Supported RADIUS Attributes | 436
Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438

Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch | 440

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

Interfaces Enabled for 802.1X or MAC RADIUS Authentication | 456

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch | 456
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication | 464
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on EX Series Switches with ELS Support | 471

Static MAC Bypass of 802.1X and MAC RADIUS Authentication | 477

Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure) | 478
Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479

Captive Portal Authentication | 485

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Configuring Captive Portal Authentication (CLI Procedure) | 492

Configuring Secure Access for Captive Portal | 492
Enabling an Interface for Captive Portal | 493
Configuring Bypass of Captive Portal Authentication | 493
Designing a Captive Portal Authentication Login Page on Switches | 494
Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switch with ELS Support | 497

Configuring Secure Access for Captive Portal | 498
Enabling an Interface for Captive Portal | 498
### Configuring Bypass of Captive Portal Authentication | 498

Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support | 499

### Flexible Authentication Order on EX Series Switches | 505

Configuring Flexible Authentication Order | 506

Configuring EAPoL Block to Maintain an Existing Authentication Session | 508

### Central Web Authentication | 510

Understanding Central Web Authentication | 510

Central Web Authentication Process | 511

Dynamic Firewall Filters for Central Web Authentication | 512

Redirect URL for Central Web Authentication | 513

Configuring Central Web Authentication | 513

Configuring Dynamic Firewall Filters for Central Web Authentication | 514

Configuring the Redirect URL for Central Web Authentication | 515

Guidelines for Configuring Central Web Authentication | 516

### Centralized Access Control to Network Resources on EX Series Switches | 517

Understanding Centralized Network Access Control and EX Series Switches | 517

NAC Using Any RADIUS Server and Access Policies Defined on the Local Switch | 518

Centralized NAC Using Junos Pulse Access Control Service | 518

Captive Portal Authentication | 519

Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520

Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523

### VoIP on EX Series Switches | 525

Understanding 802.1X and VoIP on EX Series Switches | 525

Multi Domain 802.1X Authentication | 527

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support | 537

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support | 544

Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication | 550

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support | 558
Configuring IEEE 802.1x Port-Based Network Access Control

IEEE 802.1x Port-Based Network Access Control Overview | 571

Understanding the Administrative State of the Authenticator Port | 572

Understanding the Administrative Mode of the Authenticator Port | 572

Configuring the Authenticator | 573

Viewing the dot1x Configuration | 574

Configuring IEEE 802.1x Port-Based Network Access Control in Enhanced LAN Mode

802.1X for MX Series Routers in Enhanced LAN Mode Overview | 577

How 802.1X Authentication Works | 578

802.1X Features Overview | 580

Supported Features Related to 802.1X Authentication | 580

Understanding 802.1X and LLDP and LLDP-MED on MX Series Routers in Enhanced LAN Mode | 581

Understanding 802.1X and RADIUS Accounting on MX Series Routers in Enhanced LAN Mode | 584

Understanding 802.1X and VoIP on MX Series Routers in Enhanced LAN Mode | 585

Understanding Guest VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode | 588

Understanding Dynamic VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode | 588

Understanding Server Fail Fallback and Authentication on MX Series Routers in Enhanced LAN Mode | 589

Configuring 802.1X RADIUS Accounting on MX Series Routers in Enhanced LAN Mode | 590

Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode | 593

Configuring LLDP-MED on MX Series Routers in Enhanced LAN Mode | 595

Enabling LLDP-MED on Interfaces | 595

Configuring Location Information Advertised by the Router | 595
Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server | 707
Example: Complete DHCP Server Configuration | 708
Verifying and Managing the DHCP Server Configuration | 710
Example: Viewing DHCP Bindings | 711
Example: Viewing DHCP Address Pools | 712
Example: Viewing and Clearing DHCP Conflicts | 712
Configuring Tracing Operations for DHCP Processes | 713
  Configuring the DHCP Processes Log Filename | 713
  Configuring the Number and Size of DHCP Processes Log Files | 714
  Configuring Access to the DHCP Log File | 714
  Configuring a Regular Expression for Refining the Output of DHCP Logged Events | 715
  Configuring DHCP Trace Operation Events | 715
DHCP Processes Tracing Flags | 716

Extended DHCP Local Server | 717
Extended DHCP Local Server Overview | 718
  Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 720
  Providing DHCP Client Configuration Information | 720
  Minimal Configuration for Clients | 722
  DHCP Local Server and Address-Assignment Pools | 722
Configuring the Router as an Extended DHCP Local Server | 723
Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 725
Extended DHCP Local Server and Address-Assignment Pools | 725
Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use | 726
  Matching the Client IP Address to the Address-Assignment Pool | 727
  Matching Option 82 Information to Named Address Ranges | 727
Default Options Provided by the Extended DHCP Server for the DHCP Client | 727
Using External AAA Authentication Services to Authenticate DHCP Clients | 728
  Configuring Authentication Support for an Extended DHCP Application | 728
  Grouping Interfaces with Common DHCP Configurations | 730
  Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service | 731
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring DHCP and BOOTP</td>
<td>765</td>
</tr>
<tr>
<td>Configuring DHCP and BOOTP Relay</td>
<td>766</td>
</tr>
<tr>
<td>Configuring a DHCP and BOOTP Relay Agent</td>
<td>767</td>
</tr>
<tr>
<td>Configuring DHCP Smart Relay</td>
<td>768</td>
</tr>
<tr>
<td>Graceful Routing Engine Switchover for DHCP</td>
<td>769</td>
</tr>
<tr>
<td>Centrally Configured Opaque DHCP Options</td>
<td>770</td>
</tr>
<tr>
<td>Data Flow for RADIUS-Sourced DHCP Options</td>
<td>771</td>
</tr>
<tr>
<td>Multiple VSA 26-55 Instances Configuration</td>
<td>773</td>
</tr>
<tr>
<td>DHCP Options That Cannot Be Centrally Configured</td>
<td>773</td>
</tr>
<tr>
<td>Extended DHCP Local Server</td>
<td>774</td>
</tr>
<tr>
<td>Extended DHCP Local Server Overview</td>
<td>775</td>
</tr>
<tr>
<td>Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools</td>
<td>777</td>
</tr>
<tr>
<td>Providing DHCP Client Configuration Information</td>
<td>777</td>
</tr>
<tr>
<td>Minimal Configuration for Clients</td>
<td>779</td>
</tr>
<tr>
<td>DHCP Local Server and Address-Assignment Pools</td>
<td>779</td>
</tr>
<tr>
<td>Example: Minimum Extended DHCP Local Server Configuration</td>
<td>780</td>
</tr>
<tr>
<td>Disabling Automatic Binding of Stray DHCP Requests</td>
<td>780</td>
</tr>
<tr>
<td>Configuring a Token for DHCP Local Server Authentication</td>
<td>782</td>
</tr>
<tr>
<td>Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)</td>
<td>783</td>
</tr>
<tr>
<td>Verifying and Managing DHCP Local Server Configuration</td>
<td>783</td>
</tr>
<tr>
<td>DHCPv6 Local Server</td>
<td>786</td>
</tr>
<tr>
<td>DHCPv6 Local Server Overview</td>
<td>787</td>
</tr>
<tr>
<td>Specifying the Delegated Address Pool for IPv6 Prefix Assignment</td>
<td>788</td>
</tr>
<tr>
<td>Preventing Binding of Clients That Do Not Support Reconfigure Messages</td>
<td>789</td>
</tr>
<tr>
<td>Configuring DHCPv6 Rapid Commit (MX, EX)</td>
<td>790</td>
</tr>
<tr>
<td>Verifying and Managing DHCPv6 Local Server Configuration</td>
<td>790</td>
</tr>
<tr>
<td>Extended DHCP Relay Agent</td>
<td>791</td>
</tr>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers</td>
<td>793</td>
</tr>
<tr>
<td>DHCP Liveness Detection</td>
<td>795</td>
</tr>
<tr>
<td>Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets</td>
<td>795</td>
</tr>
<tr>
<td>Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent</td>
<td>795</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Replacing the DHCP Relay Request and Release Packet Source Address</td>
<td>796</td>
</tr>
<tr>
<td>Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings</td>
<td>797</td>
</tr>
<tr>
<td>Example: Minimum JDHCPRelay Agent Configuration</td>
<td>802</td>
</tr>
<tr>
<td>Verifying and Managing DHCP Relay Configuration</td>
<td>802</td>
</tr>
<tr>
<td>Overriding the Default DHCP Relay Configuration Settings</td>
<td>803</td>
</tr>
<tr>
<td>Overriding the Default DHCP Local Server Configuration Settings Overview</td>
<td>807</td>
</tr>
<tr>
<td>Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally</td>
<td>810</td>
</tr>
<tr>
<td>DHCP Relay Agent Information Option (Option 82)</td>
<td>810</td>
</tr>
<tr>
<td>Using DHCP Relay Agent Option 82 Information</td>
<td>811</td>
</tr>
<tr>
<td>Configuring Option 82 Information</td>
<td>812</td>
</tr>
<tr>
<td>Overriding Option 82 Information</td>
<td>814</td>
</tr>
<tr>
<td>Including a Prefix in DHCP Options</td>
<td>815</td>
</tr>
<tr>
<td>Including a Textual Description in DHCP Options</td>
<td>818</td>
</tr>
<tr>
<td>How DHCP Relay Agent Uses Option 82 for Auto Logout</td>
<td>820</td>
</tr>
<tr>
<td>Enable Processing of Untrusted Packets So Option 82 Information Can Be Used</td>
<td>822</td>
</tr>
<tr>
<td>DHCP Auto Logout Overview</td>
<td>822</td>
</tr>
<tr>
<td>Auto Logout Overview</td>
<td>822</td>
</tr>
<tr>
<td>How DHCP Identifies and Releases Clients</td>
<td>823</td>
</tr>
<tr>
<td>Option 60 and Option 82 Requirements</td>
<td>824</td>
</tr>
<tr>
<td>Automatically Logging Out DHCP Clients</td>
<td>824</td>
</tr>
<tr>
<td>DHCP Relay Proxy</td>
<td>825</td>
</tr>
<tr>
<td>DHCP Relay Proxy Overview</td>
<td>826</td>
</tr>
<tr>
<td>Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers</td>
<td>826</td>
</tr>
<tr>
<td>Benefits of Using DHCP Relay Proxy</td>
<td>827</td>
</tr>
<tr>
<td>Enabling DHCP Relay Proxy Mode</td>
<td>828</td>
</tr>
<tr>
<td>DHCPv6 Relay Agent</td>
<td>828</td>
</tr>
<tr>
<td>DHCPv6 Relay Agent Overview</td>
<td>829</td>
</tr>
<tr>
<td>Inserting DHCPv6 Interface-ID Option (Option 18) in DHCPv6 Packets</td>
<td>830</td>
</tr>
<tr>
<td>Verifying and Managing DHCPv6 Relay Configuration</td>
<td>831</td>
</tr>
<tr>
<td>Managing DHCP Services on Switches</td>
<td>832</td>
</tr>
<tr>
<td>Using External AAA Authentication Services with DHCP</td>
<td>833</td>
</tr>
<tr>
<td>Creating Unique Usernames for DHCP Clients</td>
<td>834</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Specifying the Maximum Number of DHCP Clients Per Interface</td>
<td>837</td>
</tr>
<tr>
<td>DHCP Local Server Handling of Client Information Request Messages</td>
<td>838</td>
</tr>
<tr>
<td>Enabling Processing of Client Information Requests</td>
<td>839</td>
</tr>
<tr>
<td>Sending Release Messages When Clients Are Deleted</td>
<td>840</td>
</tr>
<tr>
<td>Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients</td>
<td>841</td>
</tr>
<tr>
<td>Default Client/Server Interaction</td>
<td>841</td>
</tr>
<tr>
<td>Dynamic Client/Server Interaction for DHCPv4</td>
<td>842</td>
</tr>
<tr>
<td>Dynamic Client/Server Interaction for DHCPv6</td>
<td>843</td>
</tr>
<tr>
<td>Manually Forcing the Local Server to Initiate the Reconfiguration Process</td>
<td>843</td>
</tr>
<tr>
<td>Action Taken for Events That Occur During a Reconfiguration</td>
<td>843</td>
</tr>
<tr>
<td>Benefits of Dynamic Reconfiguration of DHCP Local Server Clients</td>
<td>844</td>
</tr>
<tr>
<td>Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview</td>
<td>844</td>
</tr>
<tr>
<td>Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings</td>
<td>846</td>
</tr>
<tr>
<td>Configuring Dynamic Reconfiguration Attempts for DHCP Clients</td>
<td>847</td>
</tr>
<tr>
<td>Configuring Deletion of the Client When Dynamic Reconfiguration Fails</td>
<td>848</td>
</tr>
<tr>
<td>Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect</td>
<td>848</td>
</tr>
<tr>
<td>Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers</td>
<td>849</td>
</tr>
<tr>
<td>Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups</td>
<td>850</td>
</tr>
<tr>
<td>Grouping Interfaces and Applying a Common DHCP Configuration to the Group</td>
<td>853</td>
</tr>
<tr>
<td>Grouping Interfaces with Common DHCP Configurations</td>
<td>853</td>
</tr>
<tr>
<td>Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces</td>
<td>854</td>
</tr>
<tr>
<td>Configuring Group-Specific DHCP Local Server Options</td>
<td>856</td>
</tr>
<tr>
<td>Configuring Group-Specific DHCP Relay Options</td>
<td>856</td>
</tr>
</tbody>
</table>
DHCP Snooping | 898
DHCP Snooping Support | 898
Example: Configuring DHCP Snooping Support for DHCP Relay Agent | 900
Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | 902

DHCP for Security Devices

DHCP Overview | 909
DHCP Overview | 909
DHCP Local Server | 910
DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction | 910
DHCP Local Server and Address-Assignment Pools | 910
DHCP Client | 911
DHCP Relay Agent | 911
DHCP Client, DHCP Relay Agent, and DHCP Local Servers | 912
Considerations | 913
DHCP Settings and Restrictions Overview | 914
Propagation of TCP/IP Settings for DHCP | 914
DHCP Conflict Detection and Resolution | 914
DHCP Interface Restrictions | 914

DHCP Server | 915
Understanding DHCP Server Operation | 915
DHCP Options | 916
Compatibility with Autoinstallation | 916
Chassis Cluster Support | 916
DHCP Server Configuration Overview | 916
Minimum DHCP Local Server Configuration | 918
Enabling TCP/IP Propagation on a DHCP Local Server | 919
Example: Configuring the Device as a DHCP Server | 920
Verifying and Managing DHCP Local Server Configuration | 927

DHCP Address-Assignment Pools | 929
Configuring Address-Assignment Pools | 929
Configuring an Address-Assignment Pool Name and Addresses | 930
Configuring a Named Address Range for Dynamic Address Assignment | 930
Configuring Static Address Assignments | 931
Configuring Address-Assignment Pool Linking | 932

**DHCP Client | 933**
- Understanding DHCP Client Operation | 933
- Minimum DHCP Client Configuration | 934
- Configuring DHCP Client-Specific Attributes for Address-Assignment Pools | 934
- Configuring Optional DHCP Client Attributes | 935
- Verifying and Managing DHCP Client Configuration | 936
- Example: Configuring the Device as a DHCP Client | 937

**DHCP Relay Agent | 944**
- Understanding DHCP Relay Agent Operation | 945
- Example: Minimum JDHCP Relay Agent Configuration | 945
- Example: Configuring JDHCP Relay Configuration | 946
- Example: Configuring the Device as a BOOTP or DHCP Relay Agent using Legacy DHCP Deamon Command | 956

**DHCPv6 Server | 962**
- DHCPv6 Server Overview | 962
- Creating a Security Policy to Enable DHCPv6 Traffic | 963
- Example: Configuring DHCPv6 Server Options | 964
- Understanding Cascaded DHCPv6 Prefix Delegating | 969
- Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) | 970

**DHCPv6 Client | 996**
- DHCPv6 Client Overview | 998
- Minimum DHCPv6 Client Configuration | 998
- Configuring DHCP Client-Specific Attributes | 1000
- Configuring Optional DHCPv6 Client Attributes | 1001
- Configuring the DHCPv6 Client Rapid Commit Option | 1003
- Configuring a DHCPv6 Client in Autoconfig Mode | 1004
- Configuring TCP/IP Propagation on a DHCPv6 Client | 1005

**Understanding DHCPv6 Client and Server Identification | 1005**
DHCPv6 Address-Assignment Pools | 1007

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 1007
Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 1010
Configuring an Address-Assignment Pool for Router Advertisement | 1011
Configuring Nontemporary Address Assignment | 1012
Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 1013
Configuring Auto-Prefix Delegation | 1014

DHCP In Chassis Cluster Mode | 1015

Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode | 1015
Example: Configuring the Device as a DHCP Client in Chassis Cluster Mode | 1023

Permission Flags

access | 1035
access-control | 1040
admin | 1041
admin-control | 1047
all-control | 1048
clear | 1049
configure | 1150
control | 1151
field | 1152
firewall | 1153
firewall-control | 1159
floppy | 1160
flow-tap | 1161
flow-tap-control | 1165
flow-tap-operation | 1166
idp-profile-operation | 1167
interface | 1168
interface-control | 1173
maintenance | 1175
network | 1187
pgcp-session-mirroring | 1190
pgcp-session-mirroring-control | 1195
reset | 1196
rollback | 1197
routing | 1198
routing-control | 1209
secret | 1215
secret-control | 1221
security | 1223
security-control | 1233
shell | 1238
snmp | 1239
snmp-control | 1243
system | 1244
system-control | 1252
trace | 1255
trace-control | 1266
view | 1274
view-configuration | 1423
**Configuration Statements**

access | 1447

access (Dynamic Access Routes) | 1449

access-internal (Dynamic Access-Internal Routes) | 1451

access-profile | 1453

accounting (System) | 1455

accounting (Access Profile) | 1457

accounting (Access Profile) | 1459

accounting-options | 1461

accounting-order | 1464

accounting-port (RADIUS Server) | 1465

accounting-server | 1466

accounting-stop-on-access-deny | 1468

accounting-stop-on-failure | 1469

active-server-group | 1471

add-interface-text-description | 1473

address (Access Control Service) | 1474

address-assignment (Access) | 1475

address-assignment (Address-Assignment Pools) | 1479

address-change-immediate-update | 1482

address-pool | 1483

address-pool (Access) | 1485

address-protection | 1487

advertisement-interval | 1489

agent-address | 1491
authorization-time-interval | 1530
backoff-factor | 1532
backoff-threshold | 1533
backup-on-failure (Accounting Options) | 1534
bfd | 1535
block-interval | 1537
boot-loader-authentication | 1538
boot-server (NTP) | 1540
boot-server (NTP) | 1541
boot-server (DHCP) | 1542
broadcast | 1543
broadcast | 1545
broadcast-client | 1546
broadcast-client | 1547
ca-name | 1548
cca-type | 1549
cca-value | 1551
cache-size | 1552
ca-timeout-negative | 1553
captive-portal | 1554
certificate-verification | 1556
certificates | 1558
certification-authority | 1560
change-type | 1562
civic-based | 1563
ciphers | 1564

circuit-id (DHCP Relay Agent) | 1566

circuit-type | 1569

circuit-type (DHCP Local Server) | 1570

circuit-type (DHCP Relay Agent) | 1572

class (Defining Login Classes) | 1573

class-usage-profile | 1584

classification-key (DHCP Local Server) | 1585

classification-key (DHCP Relay Agent) | 1586

clear-on-abort (DHCP Local Server) | 1588

client-alive-count-max | 1590

client-alive-interval | 1591

client-discover-match (DHCP Local Server) | 1592

client-ia-type | 1594

client-id (DHCP Local Server) | 1595

client-id (DHCP Relay Agent) | 1596

client-identifier (DHCP Client) | 1597

client-identifier (DHCPv6 Client) | 1598

client-list-name | 1599

client-list-name (SNMP) | 1600

client-type | 1601

clients | 1602

coa-immediate-update | 1603

coa-no-override service-class-attribute | 1604

commit-delay | 1605
drop (DHCP Relay Agent Option) | 1732

dual-stack (DHCP Local Server Overrides) | 1733

dual-stack (DHCP Relay Agent Overrides) | 1734

dual-stack-group (DHCP Local Server) | 1735

dual-stack-group (DHCP Relay Agent) | 1737

dual-stack-interface-client-limit (DHCP Local Server and Relay Agent) | 1740

duplication (Access Profile) | 1741

duplication-filter (Access Profile) | 1742

duplication-vrf (Duplicate Accounting) | 1743

dynamic-pool | 1744

dynamic-profile (DHCP Local Server) | 1746

dynamic-profile (DHCP Relay Agent) | 1748

dynamic-profile-options | 1749

dynamic-server | 1750

eapol-block | 1752

elin | 1754

encoding | 1755

enhanced-accounting | 1756

enhanced-avs-max | 1757

enrollment-retry | 1758

enrollment-url | 1759

ethernet-switching-options | 1760

events | 1769

exclude (RADIUS Attributes) | 1770

excluded-address (Address-Assignment Pools) | 1778
excluded-address (Address-Assignment Pools) | 1779

external-authority | 1780

failure-action | 1781

family (Security Forwarding Options) | 1783

falling-threshold (Health Monitor) | 1784

fast-start (LLDP-MED) | 1785

fields (for Interface Profiles) | 1786

file | 1787

file (Associating with a Profile) | 1788

file (Configuring a Log File) | 1789

file (System Logging) | 1791

file (System Logging) | 1793

files | 1795

filter-duplicates | 1796

filter-profile | 1797

finger | 1798

fingerprint-hash | 1799

flow-tap-dtcp | 1800

force-discover (DHCP Client) | 1801

format (System Login) | 1802

forward-snooped-clients (DHCP Local Server) | 1803

forward-snooped-clients (DHCP Relay Agent) | 1804

forwarding-class (VoIP) | 1806

forwarding-options (Security) | 1808

ftp | 1810
interface (LLDP-MED) | 1859
interface (Static MAC Bypass) | 1861
interface (System Services DHCP) | 1862
interface (VoIP) | 1864
interface-client-limit (DHCP Local Server) | 1866
interface-client-limit (DHCP Relay Agent) | 1868
interface-delete (Subscriber Management or DHCP Client Management) | 1870
interface-description-format | 1871
interface-name (DHCP Local Server) | 1873
interface-profile | 1874
interface-traceoptions (System Services DHCP) | 1875
interfaces (ARP) | 1877
interfaces (Security Zones) | 1878
interval (Accounting Options) | 1879
interval (Access Control Service) | 1880
interval (Health Monitor) | 1881
interval (Health Monitor) | 1882
ip-address-first | 1883
keep-incoming-circuit-id (DHCP Relay Agent) | 1884
keep-incoming-remote-id (DHCP Relay Agent) | 1885
key (Authentication Keychain) | 1886
key-chain (Security) | 1888
key-exchange | 1890
layer2-liveness-detection (Send) | 1892
layer2-unicast-replies | 1894
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap-url</td>
<td>1895</td>
</tr>
<tr>
<td>lease-time</td>
<td>1896</td>
</tr>
<tr>
<td>lease-time (dhcp-client)</td>
<td>1897</td>
</tr>
<tr>
<td>liveness-detection</td>
<td>1898</td>
</tr>
<tr>
<td>lldp</td>
<td>1900</td>
</tr>
<tr>
<td>lldp</td>
<td>1902</td>
</tr>
<tr>
<td>lldp-configuration-notification-interval</td>
<td>1905</td>
</tr>
<tr>
<td>lldp-med (Ethernet Switching)</td>
<td>1906</td>
</tr>
<tr>
<td>lldp-med-bypass</td>
<td>1908</td>
</tr>
<tr>
<td>lldp-priority</td>
<td>1909</td>
</tr>
<tr>
<td>lldp-tx-fast-init</td>
<td>1910</td>
</tr>
<tr>
<td>local</td>
<td>1911</td>
</tr>
<tr>
<td>local-certificate</td>
<td>1913</td>
</tr>
<tr>
<td>local-server-group (DHCP Relay Agent Option)</td>
<td>1914</td>
</tr>
<tr>
<td>location (DHCP Relay Agent)</td>
<td>1915</td>
</tr>
<tr>
<td>location (LLDP-MED)</td>
<td>1916</td>
</tr>
<tr>
<td>location (SNMP)</td>
<td>1917</td>
</tr>
<tr>
<td>location (System)</td>
<td>1918</td>
</tr>
<tr>
<td>lockout-period</td>
<td>1920</td>
</tr>
<tr>
<td>log</td>
<td>1921</td>
</tr>
<tr>
<td>log-key-changes</td>
<td>1922</td>
</tr>
<tr>
<td>logical-system-name (DHCP Local Server)</td>
<td>1923</td>
</tr>
<tr>
<td>login</td>
<td>1924</td>
</tr>
<tr>
<td>mac-address (DHCP Local Server)</td>
<td>1927</td>
</tr>
<tr>
<td>mac-address (DHCP Relay Agent)</td>
<td>1929</td>
</tr>
</tbody>
</table>
mac-radius | 1931
macs | 1933
management-address | 1935
master-password | 1936
mau-type | 1938
max-outstanding-requests (Diameter Applications) | 1939
max-pre-authentication-packets | 1940
max-sessions-per-connection | 1941
maximum-certificates | 1942
maximum-hop-count | 1943
maximum-lease-time (DHCP) | 1944
maximum-length | 1945
maximum-lifetime | 1946
maximum-requests | 1947
maximum-time | 1948
message | 1949
method | 1950
mib-profile | 1952
minimum-changes | 1953
minimum-character-changes | 1954
minimum-interval | 1955
minimum-length | 1957
minimum-lifetime | 1958
minimum-lower-cases | 1960
minimum-numerics | 1961
minimum-punctuations | 1962
minimum-receive-interval | 1963
minimum-reuse | 1964
minimum-time | 1965
minimum-upper-cases | 1966
minimum-wait-time | 1967
multi-domain | 1968
multicast-client | 1970
multicast-client | 1971
multiplier | 1972
name-server (Access) | 1973
name-server (System Services) | 1974
nas-ip-address | 1975
nas-port-extended-format | 1976
nas-port-id-format (Subscriber Management) | 1978
nas-port-type (Subscriber Management) | 1980
neighbor-discovery-router-advertisement (Access) | 1982
neighbor-port-info-display | 1983
netbios-snooping | 1985
next-hop (Dynamic Access Routes) | 1986
next-server | 1988
no-adaptation | 1989
no-allow-snooped-clients | 1990
no-bind-on-request (DHCP Relay Agent) | 1992
no-listen | 1994
no-mac-table-binding (802.1X) | 1995
no-passwords | 1996
no-public-keys | 1997
no-reauthentication | 1998
no-tagging | 1999
no-tcp-forwarding | 2000
no-vlan-interface-name | 2001
nonpersistent | 2003
nonvolatile | 2004
ntp | 2005
object-names | 2007
oid | 2008
on-demand-address-allocation | 2009
operation | 2010
option (DHCP server) | 2011
option-60 (DHCP Local Server) | 2013
option-60 (DHCP Relay Agent) | 2014
option-82 (DHCP Local Server Authentication) | 2017
option-82 (DHCP Local Server Pool Matching) | 2019
option-82 (DHCP Relay Agent) | 2020
option-number (DHCP Relay Agent Option) | 2022
options (Access Profile) | 2024
options (Security) | 2034
order | 2035
outbound-ssh | 2037
outbound-ssh | 2042
overrides (DHCP Local Server) | 2045
overrides (DHCP Relay Agent) | 2048
overrides (DHCP Relay Agent) | 2050
overrides (System Services DHCP) | 2052
password (Login) | 2054
password (Access Control Service) | 2055
password (DHCP Local Server) | 2056
password (DHCP Relay Agent) | 2058
password (Login) | 2060
password-options | 2062
path-length | 2063
partition (Gx-Plus) | 2064
peer (NTP) | 2065
pool (DHCP Local Server Overrides) | 2066
pool (System) | 2068
pool-match-order | 2070
port (Access Control Service) | 2071
port (HTTP/HTTPS) | 2072
port (NETCONF) | 2073
port (RADIUS Server) | 2074
port (SRC Server) | 2075
port (TACACS+ Server) | 2076
port-description-type | 2077
port-id-subtype | 2079
power-negotiation | 2081
preference (Subscriber Management) | 2082
preferred-prefix-length | 2083
prefix (DHCP Client) | 2084
prefix (DHCP Relay Agent) | 2085
process-inform | 2087
profile (Access) | 2089
profile | 2096
profilerd | 2098
protocol-master | 2099
protocol-version | 2102
protocols | 2103
provisioning-order (Diameter Applications) | 2124
proxy | 2126
proxy-mode | 2127
ptopo-configuration-maximum-hold-time | 2128
ptopo-configuration-trap-interval | 2129
push-backup-to-master (Accounting Options) | 2130
quiet-period | 2131
quiet-period (Captive Portal) | 2132
radius | 2133
radius (Access Profile) | 2134
radius (System) | 2138
radius-disconnect (DHCP Local Server) | 2139
radius-options | 2141
remote-debug-permission | 2188
remote-id (DHCP Relay Agent) | 2189
replace-ip-source-with (DHCP Relay Agent) | 2192
replace-ip-source-with (DHCP Relay Agent) | 2193
req-option | 2194
retransmission-attempt (DHCP Client) | 2195
retransmission-attempt (DHCP Client) | 2196
retransmission-attempt (DHCPv6 Client) | 2197
retransmission-interval (DHCP Client) | 2198
retransmission-interval (DHCP Client) | 2199
retransmission-interval (DHCP Client) | 2200
retries (802.1X) | 2201
retries (Captive Portal) | 2202
retry | 2203
retry (RADIUS) | 2204
retry-options | 2205
revert-interval (Access) | 2206
rising-threshold (Health Monitor) | 2207
rng | 2208
root-authentication | 2209
root-login | 2211
route-suppression (DHCP Local Server and Relay Agent) | 2212
routing-engine-profile | 2214
routing-instance | 2215
routing-instance-name (DHCP Local Server) | 2216
routing-instance-name (DHCP Relay Agent) | 2218
secret (RADIUS or TACACS+ Server) | 2220
secret (RADIUS) | 2221
secret (Security) | 2222
secure-authentication | 2223
security | 2224
send-acct-status-on-config-change (Access Profile) | 2226
send-release-on-delete (DHCP Relay Agent) | 2227
server (NTP) | 2229
server (DNS, Port, and TFTP Service) | 2231
server (RADIUS Accounting) | 2233
server (TACACS+ Accounting) | 2234
server-address | 2235
server-address (dhcp-client) | 2236
server-fail | 2237
server-fail-voip | 2239
server-group | 2241
server-identifier | 2243
server-reject-vlan | 2245
server-timeout | 2247
server-timeout (Captive Portal) | 2248
servers | 2249
service (Service Accounting) | 2250
service-deployment | 2251
service-profile (DHCP Local Server) | 2252
static-subscribers | 2295
statistics (Access Profile) | 2296
statistics-service | 2297
strict (DHCP Local Server) | 2298
sub-prefix-length | 2299
subscriber-management-helper | 2300
supplicant | 2301
supplicant-timeout | 2303
system-generated-certificate | 2304
tacplus | 2305
tacplus | 2306
tacplus-options | 2308
tacplus-server | 2310
tacplus-server | 2312
targets | 2314
tcp-forwarding (JDM) | 2315
telnet | 2316
tftp | 2317
threshold (detection-time) | 2318
threshold (transmit-interval) | 2320
timeout (Access Control Service) | 2321
timeout (DHCP Local Server) | 2322
timeout (System) | 2324
timeout-action (Access Control Service) | 2325
tlv-filter | 2326
tlv-select | 2329

token (DHCP Local Server) | 2332

trace (DHCP Relay Agent) | 2334

traceoptions (802.1X) | 2336

traceoptions (Address-Assignment Pool) | 2338

traceoptions (DHCP) | 2340

traceoptions (DHCP Server) | 2343

traceoptions (DNS, Port, and TFTP Packet Forwarding) | 2347

traceoptions (LLDP) | 2350

traceoptions (LLDP) | 2353

traceoptions (Outbound SSH) | 2356

traceoptions (SBC Configuration Process) | 2358

traceoptions (Security) | 2360

transfer-interval | 2363

transmit-delay (LLDP) | 2364

transmit-delay | 2365

transmit-interval | 2367

transmit-period | 2368

trap-group | 2369

trap-options | 2371

trigger (DHCP Local Server) | 2373

tries-before-disconnect | 2375

trust-option-82 | 2376

trusted-key | 2377

uac-policy | 2378
uac-service | 2379
uac-service | 2380
unattended-boot | 2381
unified-access-control | 2382
update-interval | 2383
update-router-advertisement | 2385
update-server | 2386
update-server (dhcp-client) | 2387
update-server (dhcpv6-client) | 2388
usb-control | 2389
use-interface | 2390
use-interface-description | 2391
use-primary (DHCP Local Server) | 2394
use-primary (DHCP Relay Agent) | 2396
use-vlan-id | 2398
use-vlan-id (DHCP Relay Agent) | 2400
user (Access) | 2402
user-defined-option-82 | 2404
user-id | 2406
user-keepalive | 2407
user-prefix (DHCP Local Server) | 2408
username-include (DHCP Local Server) | 2410
username-include (DHCP Relay Agent) | 2412
vendor-id | 2414
vendor-option | 2415
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor-option</td>
<td>2416</td>
</tr>
<tr>
<td>version (BFD)</td>
<td>2418</td>
</tr>
<tr>
<td>version (SNMP)</td>
<td>2420</td>
</tr>
<tr>
<td>versioning</td>
<td>2421</td>
</tr>
<tr>
<td>view-configuration</td>
<td>2421</td>
</tr>
<tr>
<td>vlan (VoIP)</td>
<td>2423</td>
</tr>
<tr>
<td>vlan-assignment</td>
<td>2424</td>
</tr>
<tr>
<td>vlan-name-tlv-option</td>
<td>2426</td>
</tr>
<tr>
<td>voip</td>
<td>2427</td>
</tr>
<tr>
<td>vpn (Forwarding Options)</td>
<td>2428</td>
</tr>
<tr>
<td>wait-for-acct-on-ack (Access Profile)</td>
<td>2429</td>
</tr>
<tr>
<td>watchdog</td>
<td>2430</td>
</tr>
<tr>
<td>web-management</td>
<td>2431</td>
</tr>
<tr>
<td>web-management (System Processes)</td>
<td>2432</td>
</tr>
<tr>
<td>web-management (System Services)</td>
<td>2433</td>
</tr>
<tr>
<td>what</td>
<td>2438</td>
</tr>
<tr>
<td>wins-server (System)</td>
<td>2440</td>
</tr>
<tr>
<td>xnm-clear-text</td>
<td>2441</td>
</tr>
<tr>
<td>xnm-ssl</td>
<td>2442</td>
</tr>
</tbody>
</table>

### Operational Commands

- clear accounting server statistics archival-transfer | 2451
- clear captive-portal | 2452
- clear dhcp client binding | 2455
- clear dhcp client statistics | 2456
- clear dhcp relay binding | 2457
clear dhcp relay statistics | 2458
clear dhcp server binding | 2459
clear dhcp server statistics | 2460
clear dhcpv6 client binding | 2461
clear dhcpv6 client statistics | 2462
clear dhcpv6 relay binding | 2463
clear dhcpv6 relay statistics | 2467
clear dhcpv6 server binding | 2470
clear dhcpv6 server binding (Local Server) | 2473
clear dhcpv6 server statistics | 2474
clear dhcpv6 server statistics (Local Server) | 2476
clear dot1x | 2477
clear lldp neighbors | 2480
clear lldp statistics | 2481
clear lldp neighbors | 2482
clear lldp statistics | 2483
clear network-access radsec state | 2484
clear network-access radsec statistics | 2485
clear security pki local-certificate | 2486
clear security ssh key-pair-identity | 2488
clear system login lockout | 2489
clear system services dhcp binding | 2490
clear system services dhcp conflict | 2491
clear system services dhcp statistics | 2492
request component login | 2493
request dhcp client renew | 2496
request dhcp server reconfigure | 2497
request dhcpv6 server reconfigure | 2499
request dhcpv6 client renew | 2501
request ipsec switch | 2502
request message | 2503
request security certificate enroll (Signed) | 2505
request security certificate enroll (Unsigned) | 2507
request security key-pair | 2509
request security pki generate-key-pair | 2511
request security pki local-certificate generate-self-signed | 2513
request security ssh key-pair-identity generate | 2515
request security tpm master-encryption-password set | 2517
request system autorecovery state | 2519
request system decrypt password | 2522
request system download abort | 2524
request system download clear | 2526
request system download pause | 2527
request system download resume | 2529
request system download start | 2531
request system firmware upgrade | 2533
request system license update | 2535
request system reboot | 2537
request system reboot (SRX Series) | 2547
request system services dhcp | 2549
request system snapshot (Maintenance) | 2550
request system software abort in-service-upgrade (ICU) | 2554
request system software add (Maintenance) | 2556
request system software rollback (SRX Series) | 2557
request system zeroize | 2558
restart (Reset) | 2560
show accounting server statistics archival-transfer | 2565
show captive-portal authentication-failed-users | 2566
show captive-portal firewall | 2568
show captive-portal interface | 2571
show chassis routing-engine (View) | 2576
show dhcp client binding | 2582
show dhcp client statistics | 2586
show dhcp relay binding | 2590
show dhcp relay statistics | 2593
show dhcp server binding | 2595
show dhcp server statistics | 2597
show dhcpv6 client binding | 2600
show dhcpv6 client statistics | 2603
show dhcpv6 relay binding | 2606
show dhcpv6 relay statistics | 2617
show dhcpv6 server binding | 2622
show dhcpv6 server binding (View) | 2630
show dhcpv6 server statistics | 2636
show dhcpv6 server statistics (View) | 2640
show dot1x | 2644
show dot1x accounting attribute | 2651
show dot1x authentication-failed-users | 2654
show dot1x firewall | 2656
show dot1x static-mac-address | 2658
show dot1x statistics | 2660
show ethernet-switching interface | 2663
show ethernet-switching interfaces | 2667
show firewall (View) | 2677
show lldp | 2680
show lldp local-information | 2688
show lldp neighbors | 2691
show lldp neighbors | 2697
show lldp remote-global-statistics | 2705
show lldp statistics | 2707
show lldp statistics | 2709
show network-access aaa statistics accounting | 2712
show network-access aaa statistics authentication | 2714
show network-access aaa statistics dynamic-requests | 2716
show network-access radsec local-certificate | 2718
show network-access radsec statistics | 2721
show network-access radsec state | 2724
show route extensive | 2727
show route instance | 2753
show route protocol | 2758
show security ssh key-pair-identity | 2776
show security pki local-certificate | 2778
show security tpm status | 2782
show services unified-access-control authentication-table | 2784
show services unified-access-control policies | 2787
show services unified-access-control status | 2790
show snmp | 2791
show snmp statistics | 2794
show ssl-certificates | 2802
show subscribers | 2805
show system autorecovery state | 2854
show system download | 2856
show system license (View) | 2858
show system login lockout | 2862
show system services dhcp binding | 2864
show system services dhcp client | 2867
show system services dhcp conflict | 2871
show system services dhcp global | 2873
show system services dhcp pool | 2875
show system services dhcp relay-statistics | 2878
show system services dhcp statistics | 2880
show system services service-deployment | 2883
show system snapshot media | 2885
show system storage partitions | 2888
show system users | 2892
ssh | 2898

telnet | 2901

test access profile | 2904

test access radius-server | 2909
About the Documentation

The Junos operating system (Junos OS) enables you to configure user access and authentication features at the [edit system] hierarchy level of the CLI. Essential user access features include login classes, user accounts, access privilege levels, and user authentication methods. Use the topics on this page to configure essential user access features for your system.

Documentation and Release Notes

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

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

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

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the `load merge` or the `load merge relative` command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.
If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a full example. In this case, use the load merge command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

To merge a snippet, follow these steps:

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

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

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

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

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

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

For more information about the `load` command, see CLI Explorer.

### Documentation Conventions

*Table 1 on page lxii* defines notice icons used in this guide.
### Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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

### Table 2: Text and Syntax Conventions

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

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

**GUI Conventions**
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select All Interfaces.  
• To cancel the configuration, click Cancel. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select **Protocols>Ospf**. |

---

**Documentation Feedback**

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- **Online feedback system**—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:

  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- **E-mail**—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

---

**Requesting Technical Support**

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

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

**Self-Help Online Tools and Resources**

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

- **Find CSC offerings**: [https://www.juniper.net/customers/support/](https://www.juniper.net/customers/support/)
- **Search for known bugs**: [https://prsearch.juniper.net/](https://prsearch.juniper.net/)
- **Find product documentation**: [https://www.juniper.net/documentation/](https://www.juniper.net/documentation/)
- **Find solutions and answer questions using our Knowledge Base**: [https://kb.juniper.net/](https://kb.juniper.net/)
- **Download the latest versions of software and review release notes**: [https://www.juniper.net/customers/csc/software/](https://www.juniper.net/customers/csc/software/)
- **Search technical bulletins for relevant hardware and software notifications**: [https://kb.juniper.net/InfoCenter/](https://kb.juniper.net/InfoCenter/)
- **Join and participate in the Juniper Networks Community Forum**: [https://www.juniper.net/company/communities/](https://www.juniper.net/company/communities/)
- **Create a service request online**: [https://myjuniper.juniper.net](https://myjuniper.juniper.net)

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: [https://entitlementsearch.juniper.net/entitlementsearch/](https://entitlementsearch.juniper.net/entitlementsearch/)

**Creating a Service Request with JTAC**

You can create a service request with JTAC on the Web or by telephone.

- **Visit** [https://myjuniper.juniper.net](https://myjuniper.juniper.net).
- **Call** 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see [https://support.juniper.net/support/requesting-support/](https://support.juniper.net/support/requesting-support/).
Login Classes and Login Settings

Junos OS Login Classes Overview  |  69
Junos OS Login Settings  |  75
Junos OS login classes allow you to define access privileges, permission for using CLI commands and statements, and session idle time for each login class. You can apply a login class to an individual user account, thereby specifying certain privileges and permissions to the user. Read this topic for more information.

All users who can log in to the router or switch must be in a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

You can define any number of login classes and then apply one login class to an individual user account.

The Junos operating system (Junos OS) contains a few predefined login classes, which are listed in Table 3 on page 69. The predefined login classes cannot be modified.

Table 3: Predefined System Login Classes

<table>
<thead>
<tr>
<th>Login Class</th>
<th>Permission Flag Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>clear, network, reset, trace, and view</td>
</tr>
<tr>
<td>read-only</td>
<td>view</td>
</tr>
<tr>
<td>superuser or super-user</td>
<td>all</td>
</tr>
</tbody>
</table>
Table 3: Predefined System Login Classes (continued)

<table>
<thead>
<tr>
<th>Login Class</th>
<th>Permission Flag Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>unauthorized</td>
<td>None</td>
</tr>
</tbody>
</table>

NOTE:

- You cannot modify a predefined login class name. If you issue the `set` command on a predefined class name, the Junos OS appends `-local` to the login class name. The following message also appears:

```
warning: '<class-name>' is a predefined class name; changing to '<class-name>-local'
```

- You cannot issue the `rename` or `copy` command on a predefined login class. Doing so results in the following error message:

```
error: target '<class-name>' is a predefined class
```

Permission Bits

Each top-level CLI command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission bits (see Table 4 on page 70).

Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is `interface`.
- Form that ends in `-control`—Provides read and write capability for that permission type. An example is `interface-control`.

Table 4: Permission Bits for Login Classes

<table>
<thead>
<tr>
<th>Permission Bit</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Can view user account information in configuration mode and with the <code>show configuration</code> command.</td>
</tr>
<tr>
<td>admin-control</td>
<td>Can view user accounts and configure them (at the [edit system login] hierarchy level).</td>
</tr>
</tbody>
</table>
Table 4: Permission Bits for Login Classes (continued)

<table>
<thead>
<tr>
<th>Permission Bit</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td>Can view the access configuration in configuration mode and with the <strong>show configuration</strong> operational mode command.</td>
</tr>
<tr>
<td>access-control</td>
<td>Can view and configure access information (at the [edit access] hierarchy level).</td>
</tr>
<tr>
<td>all</td>
<td>Has all permissions.</td>
</tr>
<tr>
<td>clear</td>
<td>Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands).</td>
</tr>
<tr>
<td>configure</td>
<td>Can enter configuration mode (using the <strong>configure</strong> command) and commit configurations (using the <strong>commit</strong> command).</td>
</tr>
<tr>
<td>control</td>
<td>Can perform all control-level operations (all operations configured with the -control permission bits).</td>
</tr>
<tr>
<td>field</td>
<td>Reserved for field (debugging) support.</td>
</tr>
<tr>
<td>firewall</td>
<td>Can view the firewall filter configuration in configuration mode.</td>
</tr>
<tr>
<td>firewall-control</td>
<td>Can view and configure firewall filter information (at the [edit firewall] hierarchy level).</td>
</tr>
<tr>
<td>floppy</td>
<td>Can read from and write to the removable media.</td>
</tr>
<tr>
<td>interface</td>
<td>Can view the interface configuration in configuration mode and with the <strong>show configuration</strong> operational mode command.</td>
</tr>
<tr>
<td>interface-control</td>
<td>Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces (at the [edit] hierarchy).</td>
</tr>
<tr>
<td>maintenance</td>
<td>Can perform system maintenance, including starting a local shell on the device and becoming the superuser in the shell (by issuing the <strong>su root</strong> command), and can halt and reboot the device (using the <strong>request system</strong> commands).</td>
</tr>
<tr>
<td>network</td>
<td>Can access the network by entering the ping, ssh, telnet, and traceroute commands.</td>
</tr>
<tr>
<td>reset</td>
<td>Can restart software processes using the <strong>restart</strong> command and can configure whether software processes are enabled or disabled (at the [edit system processes] hierarchy level).</td>
</tr>
</tbody>
</table>
Table 4: Permission Bits for Login Classes *(continued)*

<table>
<thead>
<tr>
<th>Permission Bit</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>rollback</td>
<td>Can use the <code>rollback</code> command to return to a previously committed configuration other than the most recently committed one.</td>
</tr>
<tr>
<td>routing</td>
<td>Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.</td>
</tr>
<tr>
<td>routing-control</td>
<td>Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the <code>[edit routing-options]</code> hierarchy level), routing protocols (at the <code>[edit protocols]</code> hierarchy level), and routing policy (at the <code>[edit policy-options]</code> hierarchy level).</td>
</tr>
<tr>
<td>secret</td>
<td>Can view passwords and other authentication keys in the configuration.</td>
</tr>
<tr>
<td>secret-control</td>
<td>Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.</td>
</tr>
<tr>
<td>security</td>
<td>Can view security configuration in configuration mode and with the <code>show configuration</code> operational mode command.</td>
</tr>
<tr>
<td>security-control</td>
<td>Can view and configure security information (at the <code>[edit security]</code> hierarchy level).</td>
</tr>
<tr>
<td>shell</td>
<td>Can start a local shell on the device by entering the <code>start shell</code> command.</td>
</tr>
<tr>
<td>snmp</td>
<td>Can view SNMP configuration information in configuration and operational modes.</td>
</tr>
<tr>
<td>snmp-control</td>
<td>Can view SNMP configuration information and configure SNMP (at the <code>[edit snmp]</code> hierarchy level).</td>
</tr>
<tr>
<td>system</td>
<td>Can view system-level information in configuration and operational modes.</td>
</tr>
<tr>
<td>system-control</td>
<td>Can view system-level configuration information and configure it (at the <code>[edit system]</code> hierarchy level).</td>
</tr>
<tr>
<td>trace</td>
<td>Can view trace file settings in configuration and operational modes.</td>
</tr>
<tr>
<td>trace-control</td>
<td>Can view trace file settings and configure trace file properties.</td>
</tr>
<tr>
<td>view</td>
<td>Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics.</td>
</tr>
</tbody>
</table>
Denying or Allowing Individual Commands

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that are otherwise permitted or not allowed by a permission bit.

Defining Junos OS Login Classes

Login classes allow you to define the following:

- Access privileges that users have when they are logged in to the router or switch
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

All users who can log in to the router or switch must be in a login class. Therefore, you must define a Junos OS login class for each user or class of users. You can define any number of login classes depending on the types of permissions the users need.

To define a login class and its access privileges, include the class statement at the [edit system login] hierarchy level:

```plaintext
[edit system login]
class class-name {
    access-end hh:mm;
    access-start hh:mm;
    ( allow-commands | allow-commands-regexps ) "regular expression 1" "regular expression 2";
    ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular expression 2";
    allow-sources [ allow-sources ... ];
    allow-times [ allow-times ... ];
    allowed-days [ days of the week ];
    cli {
        prompt prompt;
    }
    configuration-breadcrumbs;
    confirm-commands [ "regular expression or command 1" "regular expression or command 2" ... ] {
        confirmation-message;
    }
    ( deny-commands | deny-commands-regexps ) [ "regular expression 1" "regular expression 2" ... ];
    ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular expression 2";
    deny-sources [ deny-sources ... ];
}
```
Example: Creating Login Classes with Specific Privileges

Login classes are used to assign certain permissions or restrictions to groups of users, ensuring that sensitive commands are only accessible to the appropriate users. By default, Juniper Networks devices have four types of login classes with preset permissions: operator, read-only, superuser or super-user, and unauthorized.

You can create new custom login classes to make different combinations of permissions that are not found in the default login classes. The following example shows how to create three custom login classes, each with specific privileges and timers to disconnect the class members after a period of inactivity. Inactivity timers help protect network security by disconnecting a user from the network if the user is away from his computer for too long, preventing potential security risks created by leaving an unattended account logged in to a switch or router. The permissions and inactivity timers shown here are only examples and should be customized to your organization.

The first class of users is called observation and they can only view statistics and configuration. They are not allowed to modify any configuration. The second class of users is called operation and they can view and modify the configuration. The third class of users is called engineering and they have unlimited access and control. All three login classes use the same inactivity timer of 5 minutes.

```plaintext
[edit]
system {
    login {
        class observation {
            idle-timeout 5;
            permissions [ view ];
        }
    }
}
```
class operation {
    idle-timeout 5;
    permissions [ admin clear configure interface interface-control network reset routing routing-control snmp snmp-control trace-control firewall-control rollback ];
}
class engineering {
    idle-timeout 5;
    permissions all;
}

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Junos OS User Accounts</th>
<th>91</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos OS Administrative Roles</td>
<td>105</td>
</tr>
<tr>
<td>Junos OS User Access Privileges</td>
<td>117</td>
</tr>
</tbody>
</table>

Junos OS Login Settings

IN THIS SECTION

- Configuring Junos OS to Display a System Login Announcement | 76
- Configuring System Alarms to Appear Automatically Upon Login | 78
- Configuring Login Tips | 78
- Examples: Configuring Time-Based User Access | 79
- Configuring the Timeout Value for Idle Login Sessions | 80
- Login Retry Options | 81
- Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82
- Example: Configuring Login Retry Options | 84
Junos OS allows you to specify various settings for the users after they have logged in. You can define what to notify for the users after they have logged in, display system alarms, provide login tips, or specify time-based user access, and limit the number of login attempts. Read this topic for more information.

Configuring Junos OS to Display a System Login Announcement

Sometimes you want to make announcements only to authorized users after they have logged in. For example, you might want to announce an upcoming maintenance event.

You can format the announcement using the following special characters:

- \n—New line
- \t—Horizontal tab
- ’—Single quotation mark
- “—Double quotation mark
- \—Backslash

If the message text contains any spaces, enclose it in quotation marks.

By default, no login announcement is displayed.

To configure an announcement that can be seen only by authorized users:

1. Include the announcement statement in the [edit system login] configuration.

```
[edit system login]
user@host# set announcement text
```

For example:

```
system {
    login {
        announcement "\tJuly 27th 1:00 AM to 8:00\n\nPlanned Network Maintenance\nAFFECTED LOCATIONS: Sunnyvale\nPLANNED ACTIVITY: Upgrade all 6200 switch firmware to the Enterprise TAC recommended firmware version\nPURPOSE: This activity will help to minimize the impact of unplanned power outages as well as address known issues within our currently installed firmware version(s)\nWHAT TO EXPECT: During the maintenance window for your site, the office network will not be available.\n";
message "\n\tTP0 - M7i - IX Router Lab\n\tUNAUTHORIZED USE OF THIS ROUTER IS STRICTLY PROHIBITED!\n\tPlease contact \astatti@juniper.net\ to gain access to this equipment if you need authorization."
```
2. Commit the configuration.

```
[edit system login]
user@host# commit
```

3. Connect to the device in a new session to verify the presence of the new banner.

The preceding login message configuration example produces a login message similar to the following:

```
server% telnet host
Trying 203.0.113.0
Connected to host.example.net
Escape character is '^]'.

TP0 - M7i - iX Router Lab

UNAUTHORIZED USE OF THIS ROUTER IS STRICTLY PROHIBITED!

Please contact 'astatti@juniper.net' to gain access to this equipment if you need authorization

login: user
Password:

July 27th 1:00 AM to 8:00

Planned Network Maintenance

AFFECTED LOCATIONS: Sunnyvale

PLANNED ACTIVITY: Upgrade all 6200 switch firmware to the Enterprise TAC recommended firmware version

PURPOSE: This activity will help to minimize the impact of unplanned power
outages as well as address known issues within our currently installed firmware version(s)

WHAT TO EXPECT: During the maintenance window for your site, the office network will not be available.

If the announcement text contains any spaces, enclose the text in quotation marks.

A system login announcement appears after the user logs in. A system login message appears before the user logs in.

**TIP:** You can use the same special characters described to format your system login announcement.

---

### Configuring System Alarms to Appear Automatically Upon Login

You can configure Juniper Networks routers and switches to run the `show system alarms` command whenever a user with the login class `admin` logs in to the router or switch. To do so, include the `login-alarms` statement at the `[edit system login class admin]` hierarchy level.

```
[edit system login class admin]
login-alarms;
```

For more information on the `show system alarms` command, see the [CLI Explorer](#).

---

**SEE ALSO**

- `show system alarms`

---

### Configuring Login Tips

The Junos OS CLI provides the option of configuring login tips for the user. By default, the `tip` command is not enabled when a user logs in.
To enable tips, include the `login-tip` statement at the `[edit system login class class-name]` hierarchy level:

```
[edit system login class class-name]
login-tip;
```

Adding this statement enables the `tip` command for the class specified, provided the user logs in using the CLI.

### Examples: Configuring Time-Based User Access

The following example shows how to configure user access for the `operator-round-the-clock-access` login class from Monday through Friday without any restriction on access time or duration of login:

```
[edit system]
login {
    class operator-round-the-clock-access {
        allowed-days [monday tuesday wednesday thursday friday];
    }
}
```

The following example shows how to configure user access for the `operator-day-shift` login class on Monday, Wednesday, and Friday from 8:30 AM to 4:30 PM:

```
[edit system]
login {
    class operator-day-shift {
        allowed-days [monday wednesday friday];
        access-start 0830;
        access-end 1630;
    }
}
```

Alternatively, you can also specify the login start time and end time for the `operator-day-shift` login class to be from 8:30 AM to 4:30 PM in the following format:

```
[edit system]
login {
    class operator-day-shift {
        allowed-days [monday wednesday friday];
        access-start 08:30am;
        access-end 04:30pm;
    }
}
```
The following example shows how to configure user access for the operator-day-shift-all-days-of-the-week login class to be on all days of the week from 8:30 AM to 4:30 PM:

```
[edit system]
login {
    class operator-day-shift-all-days-of-the-week {
        access-start 0830;
        access-end 1630;
    }
}
```

SEE ALSO

- Configuring Time-Based User Access

### Configuring the Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the router or switch, even if that session is idle. To close idle sessions automatically, you must configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes. **Idle-timeout** can only be configured for user defined classes. Configuration won't work for the system predefined classes: operator, read-only, super-user. These classes' values and permissions are not editable.

To define the timeout value for idle login sessions, include the `idle-timeout` statement at the `[edit system login class class-name]` hierarchy level:

```
[edit system login class class-name]
idle-timeout minutes;
```

Specify the number of minutes that a session can be idle before it is automatically closed.

If you have configured a timeout value, the CLI displays messages similar to the following when timing out an idle user. It starts displaying these messages 5 minutes before timing out the user.
user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

If you configure a timeout value, the session closes after the specified time has elapsed, unless the user is running telnet or monitoring interfaces using the `monitor interface` or `monitor traffic` command.

### Login Retry Options

The security administrator can configure the number of times a user can try to log in to the device with invalid login credentials. The device can be locked after the specified number of unsuccessful authentication attempts. This helps to protect the device from malicious users attempting to access the system by guessing an account's password. The security administrator can unlock the user account or define a time period for the user account to remain locked.

The system **lockout-period** defines the amount of time the device can be locked for a user account after a specified number of unsuccessful login attempts.

The security administrator can configure a period of time after which an inactive session will be locked and require re-authentication to be unlocked. This helps to protect the device from being idle for a long period before the session times out.

The system **idle-timeout** defines length of time the CLI operational mode prompt remains active before the session times out.

The security administrator can configure a banner with an advisory notice to be displayed before the identification and authentication screen.

The system **message** defines the system login message. This message appears before a user logs in.

The number of reattempts the device allows is defined by the **tries-before-disconnect** option. The device allows 3 unsuccessful attempts by default or as configured by the administrator. The device prevents the locked users to perform activities that require authentication, until a security administrator manually clears the lock or the defined time period for the device to remain locked has elapsed. However, the existing locks are ignored when the user attempts to log in from the local console.
NOTE: To clear the console during an administrator-initiated logout, the administrator must configure the `set system login message "message string"` such that, the message-string contains newline (\n) characters and a login banner message at the end of the \n characters.

To ensure that configuration information is cleared completely, the administrator can enter 50 or more \n characters in the `message-string` of the command `set system login message "message string"`.

For example, `set system login message "Welcome to Junos!!!"`

---

**Limiting the Number of User Login Attempts for SSH and Telnet Sessions**

You can limit the number of times a user can attempt to enter a password while logging in through SSH or Telnet. The connection is terminated if a user fails to log in after the number of attempts specified. You can also specify a delay, in seconds, before a user can try to enter a password after a failed attempt. In addition, you can specify the threshold for the number of failed attempts before the user experiences a delay in being able to enter a password again.

To specify the number of times a user can attempt to enter a password while logging in, include the `retry-options` statement at the `[edit system login]` hierarchy level:

```
[edit system login]
retry-options {
  tries-before-disconnect number;
  backoff-threshold number;
  backoff-factor seconds;
  maximum-time seconds
  minimum-time seconds;
}
```

You can configure the following options:
• **tries-before-disconnect**—Number of times a user can attempt to enter a password when logging in. The connection closes if a user fails to log in after the number specified. The range is from 1 through 10, and the default is 10.

• **backoff-threshold**—Threshold for the number of failed login attempts before the user experiences a delay in being able to enter a password again. Use the **backoff-factor** option to specify the length of the delay in seconds. The range is from 1 through 3, and the default is 2.

• **backoff-factor**—Length of time, in seconds, before a user can attempt to log in after a failed attempt. The delay increases by the value specified for each subsequent attempt after the threshold. The range is from 5 through 10, and the default is 5 seconds.

• **maximum-time**—Maximum length of time, in seconds, that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured **maximum-time**, the connection is closed. The range is from 20 through 300 seconds, and the default is 120 seconds.

• **minimum-time**—Minimum length of time, in seconds, that a connection remains open while a user is attempting to enter a correct password. The range is from 20 through 60, and the default is 40.

The following example shows how to limit the user to four attempts when the user enters a password while logging in through SSH or Telnet:

```
[edit]
system [  
  login [  
    retry-options [  
      backoff-threshold 2;  
      backoff-factor 5;  
      minimum-time 40;  
      tries-before-disconnect 4;  
    ]  
  ]  
]  
```

Limiting the number of SSH and Telnet login attempts per user is one of the most effective methods of stopping brute force attacks from compromising your network security. Brute force attackers execute a large number of login attempts in a short period of time to illegitimately gain access to a private network. By configuring the **retry-options** command, you can create an increasing delay after each failed login attempt, eventually disconnecting any user who passes your set threshold of login attempts.

Set the **backoff-threshold** to 2, the **back-off-factor** to 5 seconds, and the **minimum-time** to 40 seconds. The user experiences a delay of 5 seconds after the second attempt to enter a correct password fails. After each subsequent failed attempt, the delay increases by 5 seconds. After the fourth and final failed attempt to enter a correct password, the user experiences an additional 10-second delay, and the connection closes after a total of 40 seconds.

The additional variables **maximum-time** and **lockout-period** are not set in this example.
NOTE: This sample only shows the portion of the [edit system login] hierarchy level being modified.

Example: Configuring Login Retry Options

IN THIS SECTION
- Requirements | 84
- Overview | 84
- Configuration | 86
- Verification | 87

This example shows how to configure system retry options to protect the device from malicious users.

Requirements

Before you begin, you should understand "Login Retry Options" on page 81.

No special configuration beyond device initialization is required before configuring this feature.

Overview

Malicious users sometimes try to log in to a secure device by guessing an authorized user account’s password. Locking out a user account after a number of failed authentication attempts helps protect the device from malicious users.

Device lockout allows you to configure the number of failed attempts before the user account is locked out of the device and configure the amount of time before the user can attempt to log in to the device again. You can configure the amount of time in-between failed login attempts of a user account and can manually lock and unlock user accounts.
NOTE:

This example includes the following settings:

- **backoff-factor** — Sets the length of delay in seconds after each failed login attempt. When a user incorrectly logs in to the device, the user must wait the configured amount of time before attempting to log in to the device again. The length of delay increases by this value for each subsequent login attempt after the value specified in the `backoff-threshold` statement. The default value for this statement is five seconds, with a range of five to ten seconds.

- **backoff-threshold** — Sets the threshold for the number of failed login attempts on the device before the user experiences a delay when attempting to reenter a password. When a user incorrectly logs in to the device and hits the threshold of failed login attempts, the user experiences a delay that is set in the `backoff-factor` statement before attempting to log in to the device again. The default value for this statement is two, with a range of one through three.

- **lockout-period** — Sets the amount of time in minutes before the user can attempt to log in to the device after being locked out due to the number of failed login attempts specified in the `tries-before-disconnect` statement. When a user fails to correctly login after the number of allowed attempts specified by the `tries-before-disconnect` statement, the user must wait the configured amount of minutes before attempting to log in to the device again. The lockout-period must be greater than zero. The range at which you can configure the lockout-period is one through 43,200 minutes.

- **tries-before-disconnect** — Sets the maximum number of times the user is allowed to enter a password to attempt to log in to the device through SSH or Telnet. When the user reaches the maximum number of failed login attempts, the user is locked out of the device. The user must wait the configured amount of minutes in the `lockout-period` statement before attempting to log back in to the device. The `tries-before-disconnect` statement must be set when the `lockout-period` statement is set; otherwise, the `lockout-period` statement is meaningless. The default number of attempts is ten, with a range of one through ten attempts.

Once a user is locked out of the device, if you are the security administrator, you can manually remove the user from this state using the `clear system login lockout <username>` command. You can also use the `show system login lockout` command to view which users are currently locked out, when the lockout period began for each user, and when the lockout period ends for each user.

If the security administrator is locked out of the device, he can log in to the device from the console port, which ignores any user locks. This provides a way for the administrator to remove the user lock on their own user account.

In this example the user waits for the `backoff-threshold` multiplied by the `backoff-factor` interval, in seconds, to get the login prompt. In this example, the user must wait 5 seconds after the first failed login attempt and 10 seconds after the second failed login attempt to get the login prompt. The user gets
disconnected after 15 seconds after the third failed attempt because the \texttt{tries-before-disconnect} option is configured as 3.

The user cannot attempt another login until 120 minutes has elapsed, unless a security administrator manually clears the lock sooner.

\textbf{Configuration}

\textbf{CLI Quick Configuration}

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the \texttt{[edit]} hierarchy level, and then enter \texttt{commit} from configuration mode.

\begin{Verbatim}
set system login retry-options backoff-factor 5
set system login retry-options backoff-threshold 1
set system login retry-options lockout-period 120
set system login retry-options tries-before-disconnect 3
\end{Verbatim}

\textbf{Step-by-Step Procedure}

To configure system retry-options:

1. Configure the backoff factor.

   \begin{Verbatim}
   [edit]
   user@host\# set system login retry-options backoff-factor 5
   \end{Verbatim}

2. Configure the backoff threshold.

   \begin{Verbatim}
   [edit]
   user@host\# set system login retry-options backoff-threshold 1
   \end{Verbatim}

3. Configure the amount of time the device gets locked after failed attempts.

   \begin{Verbatim}
   [edit]
   user@host\# set system login retry-options lockout-period 5
   \end{Verbatim}

4. Configure the number of unsuccessful attempts during which, the device can remain unlocked.

   \begin{Verbatim}
   [edit]
   user@host\# set system login retry-options tries-before-disconnect 3
   \end{Verbatim}
Results
From configuration mode, confirm your configuration by entering the `show system login retry-options` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login retry-options
backoff-factor 5;
backoff-threshold 1;
lockout-period 5;
tries-before-disconnect 3;
```

Confirm that the configuration is working properly.

If you are done configuring the device, enter `commit` from configuration mode.

Verification

**Displaying the Locked User Logins**

**Purpose**
Verify that the login lockout configuration is enabled.

**Action**
Attempt three unsuccessful logins for a particular username. The device will be locked for that username; then log in to the device with a different username. From operational mode, enter the `show system login lockout` command.

**Meaning**
When you perform three unsuccessful login attempts with a particular username, the device is locked for that user for five minutes, as configured in the example. You can verify that the device is locked for that user by logging in to the device with a different username and entering the `show system login lockout` command.

RELATED DOCUMENTATION

- Junos OS Login Classes Overview | 69
- Junos OS User Accounts | 91
User Accounts

Junos OS User Accounts | 91
Junos OS Administrative Roles | 105
Junos OS User Access Privileges | 117
Junos OS User Accounts

IN THIS SECTION

- Junos OS User Accounts Overview | 91
- Junos-FIPS Crypto Officer and User Accounts Overview | 93
- Example: Configuring User Accounts | 94
- Example: Configuring New Users | 95
- Configuring Junos OS User Accounts by Using a Configuration Group | 102

Junos OS allows you to create accounts for router, switch, and security users. All users also belong to one of the system login classes.

Junos OS requires that all users have a predefined user account before they can log in to the device. For each user account, you define the login name for the user and, optionally, information that identifies the user. User accounts provide a way for users to access a router or switch or security device. Read this topic for more information.

Junos OS User Accounts Overview

User accounts provide one way for users to access the device. (Users can access the device without accounts if you configured RADIUS or TACACS+ servers, as described in “Junos OS User Authentication Methods” on page 209.) For each account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

For each user account, you can define the following:

- Username: Name that identifies the user. It must be unique within the device. Do not include spaces, colons, or commas in the username. The username can be up to 64 characters long.

- User’s full name: (Optional) If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

- User identifier (UID): (Optional) Numeric identifier that is associated with the user account name. The identifier must be in the range from 100 through 64,000 and must be unique within the device. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.
You must ensure that the UID is unique. However, it is possible to assign the same UID to different users. If you do this, the CLI displays a warning when you commit the configuration and then assigns the duplicate UID.

- User’s access privilege: (Required) One of the login classes you defined in the class statement at the [edit system login] hierarchy level, or one of the default classes listed in "Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies" on page 128.

- Authentication method or methods and passwords that the user can use to access the device—(Optional) You can use SSH or a Message Digest 5 (MD5) password, or you can enter a plain-text password that the Junos OS encrypts using MD5-style encryption before entering it in the password database. For each method, you can specify the user’s password. If you configure the plain-text-password option, you are prompted to enter and confirm the password:

  ```
  [edit system login user username]
  user@host# set authentication plain-text-password
  New password: type password here
  Retype new password: retype password here
  ```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long.
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Valid passwords must contain at least one change of case or character class.

Junos-FIPS and Common Criteria have special password requirements. FIPS and Common Criteria passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the device, you cannot configure passwords unless they meet this standard.

For SSH authentication, you can copy the contents of an SSH key file into the configuration or directly configure SSH key information. Use the load-key-file URL filename command to load an SSH key file that was previously generated, e.g. by using ssh-keygen. The URL filename is the path to the file’s location and name. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys. The contents of the SSH key file are copied into the configuration immediately after you enter the load-key-file statement. Optionally, you can use the ssh-dsa public key <from hostname> and the ssh-rsa public key <from hostname> statements to directly configure SSH keys.

For each user account and for root logins, you can configure more than one public RSA or DSA key for user authentication. When a user logs in using a user account or as root, the configured public keys are referenced to determine whether the private key matches any of them.
To view the SSH keys entries, use the configuration mode `show` command. For example:

```
[edit system login user boojum]
user@host# set authentication load-key-file my-host:.ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
user@host# show
root-authentication {
    ssh-rsa "$ABC123"; # SECRET-DATA
}
```

An account for the user `root` is always present in the configuration. You configure the password for `root` using the `root-authentication` statement, as described in “Configuring the Root Password” on page 177.

---

**Junos-FIPS Crypto Officer and User Accounts Overview**

Junos-FIPS defines a restricted set of user roles. Unlike the Junos OS, which enables a wide range of capabilities to users, FIPS 140-2 defines specific types of users (Crypto Officer, User, and Maintenance). Crypto Officers and FIPS Users perform all FIPS-related configuration tasks and issue all FIPS-related commands. Crypto Officer and FIPS User configurations must follow FIPS 140-2 guidelines. Typically, no user besides a Crypto Officer can perform FIPS-related tasks.

**Crypto Officer User Configuration**

Junos-FIPS offers finer control of user permissions than those mandated by FIPS 140-2. For FIPS 140-2 conformance, any Junos-FIPS user with the `secret`, `security`, and `maintenance` permission bits set is a Crypto Officer. In most cases, the `super-user` class should be reserved for a Crypto Officer. A FIPS User can be defined as any Junos-FIPS user that does not have the `secret`, `security`, and `maintenance` bits set.

**FIPS User Configuration**

A Crypto Officer sets up FIPS Users. FIPS Users can be granted permissions normally reserved for a Crypto Officer; for example, permission to zeroize the system and individual AS-II FIPS PICs.
Example: Configuring User Accounts

The following example shows how to create accounts for four router or switch users, and create an account for the template user `remote`. All users use one of the default system login classes. User `alexander` also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
 system {
  login {
    user philip {
      full-name "Philip of Macedonia";
      uid 1001;
      class super-user;
      authentication {
        encrypted-password "$ABC123";
      }
    }
    user alexander {
      full-name "Alexander the Great";
      uid 1002;
      class view;
      authentication {
        encrypted-password "$ABC123";
        ssh-dsa "8924 37 5678 5678@gaugamela.per";
        ssh-dsa "6273 94 9283@boojum.per";
      }
    }
    user darius {
      full-name "Darius King of Persia";
      uid 1003;
      class operator;
      authentication {
        ssh-rsa "1024 37 12341234@ebatana.per";
      }
    }
    user anonymous {
      class unauthorized;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class read-only;
    }
  }
}
```
Example: Configuring New Users

This example shows how to configure new users.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

You can add new users to the device's local database. For each account, you define a login name and password for the user and specify a login class for access privileges. The login password must meet the following criteria:

- The password must be at least six characters long.
- You can include most character classes in a password (alphabetic, numeric, and special characters), but not control characters.
- The password must contain at least one change of case or character class.

In this example, you create a login class named operator-and-boot and allow it to reboot the device. You can define any number of login classes. You then allow the operator-and-boot login class to use commands defined in the clear, network, reset, trace, and view permission bits.

Then you create user accounts. User accounts enable you to access the device. (You can access the device without accounts if you configured RADIUS or TACACS+ servers.) You set the username as cmartin and the login class as superuser. Finally, you define the encrypted password for the user.
Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system login class operator-and-boot allow-commands "request system reboot"
set class system login operator-and-boot permissions [clear network reset trace view]
set system login user cmartin class superuser authentication encrypted-password $1$ABC123
```

GUI Step-by-Step Procedure
To configure new users:

1. In the J-Web user interface, select Configure>System Properties>User Management.

2. Click Edit. The Edit User Management dialog box appears.

3. Select the Users tab.

4. Click Add to add a new user. The Add User dialog box appears.

5. In the Username box, type a unique name for the user.
   
   Do not include spaces, colons, or commas in the username.

6. In the UserID box, type a unique ID for the user.

7. In the Full Name box, type the user's full name.
   
   If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.

8. In the Password and Confirm Password boxes, enter a login password for the user and verify your entry.

9. From the Login Class list, select the user's access privilege:
   
   • operator
   
   • read-only
   
   • unauthorized
   
   This list also includes any user-defined login classes.
10. Click OK in the Add User dialog box and Edit User Management dialog box.

11. Click OK to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click Commit Options>Commit.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure new users:

1. Set the name of the login class and allow the use of the reboot command.

   ```
   [edit system login]
   user@host# set class operator-and-boot allow-commands "request system reboot"
   ```

2. Set the permission bits for the login class.

   ```
   [edit system login]
   user@host# set class operator-and-boot permissions [clear network reset trace view]
   ```

3. Set the username, login class, and encrypted password for the user.

   ```
   [edit system login]
   user@host# set user cmartin class superuser authentication encrypted-password $1$ABC123
   ```

Results

From configuration mode, confirm your configuration by entering the show system login command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
  class operator-and-boot {
    permissions [ clear network reset trace view ];
    allow-commands "request system reboot";
  }
  user cmartin {
    class superuser;
  }
```
The following example shows how to create accounts for four router or switch users, and create an account for the template user `remote`. All users use one of the default system login classes. User `alexander` also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```conf
[edit]
  system {
    login {
      user philip {
        full-name "Philip of Macedonia";
        uid 1001;
        class super-user;
        authentication {
          encrypted-password "$ABC123";
        }
      }
      user alexander {
        full-name "Alexander the Great";
        uid 1002;
        class view;
        authentication {
          encrypted-password "$ABC123";
          ssh-dsa "8924 37 5678 5678@gaugamela.per";
          ssh-dsa "6273 94 9283@boojum.per";
        }
      }
      user darius {
        full-name "Darius King of Persia";
        uid 1003;
        class operator;
        authentication {
          ssh-rsa "1024 37 12341234@ecbatana.per";
        }
      }
      user anonymous {
        class unauthorized;
      }
      user remote {
        full-name "All remote users";
        uid 9999;
      }
    }
  }
```
The following example shows how to create accounts for four router or switch users, and create an account for the template user `remote`. All users use one of the default system login classes. User `alexander` also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```conf
[edit]
  system {
    login {
      user philip {
        full-name "Philip of Macedonia";
        uid 1001;
        class super-user;
        authentication {
          encrypted-password "$ABC123";
        }
      }
      user alexander {
        full-name "Alexander the Great";
        uid 1002;
        class view;
        authentication {
          encrypted-password "$ABC123";
          ssh-dsa "89243756785678@gaugamela.per";
          ssh-dsa "6273949283@boojum.per";
        }
      }
      user darius {
        full-name "Darius King of Persia";
        uid 1003;
        class operator;
        authentication {
          ssh-rsa "1024 37 12341234@ecbatana.per";
        }
      }
      user anonymous {
        class unauthorized;
      }
      user remote {
        full-name "All remote users";
        uid 9999;
      }
    }
  }
```
The following example shows how to create accounts for four router or switch users, and create an account for the template user remote. All users use one of the default system login classes. User alexander also has two digital signal algorithm (DSA) public keys configured for SSH authentication.

```
[edit]
  system {
    login {
      user philip {
        full-name "Philip of Macedonia";
        uid 1001;
        class super-user;
        authentication {
          encrypted-password "$ABC123";
        }
      }
      user alexander {
        full-name "Alexander the Great";
        uid 1002;
        class view;
        authentication {
          ssh-dsa "89243756785678@gaugamela.per";
          ssh-dsa "6273949283@boojum.per";
        }
      }
      user darius {
        full-name "Darius King of Persia";
        uid 1003;
        class operator;
        authentication {
          ssh-rsa "10243712341234@ecbatana.per";
        }
      }
      user anonymous {
        class unauthorized;
      }
      user remote {
        full-name "All remote users";
        uid 9999;
      }
    }
  }
```
If you are done configuring the device, enter **commit** from configuration mode.

**NOTE:** To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a user template account. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 239.
- Configure a user. See "Example: Configuring New Users" on page 95.
- Configure template accounts. See "Example: Creating Template Accounts" on page 213.

**Verification**

Confirm that the configuration is working properly.

**Verifying the New Users Configuration**

**Purpose**

Verify that the new users have been configured.

**Action**

From operational mode, enter the **show system login** command.
Configuring Junos OS User Accounts by Using a Configuration Group

Junos OS requires that all users have a predefined user account before they can access a router or switch. For each user account, you define the login name for the user and, optionally, information that identifies the user. After you have created an account, the software creates a home directory for the user.

It is a common practice to use remote authentication servers to centrally store information about users. Even so, it is also a good practice to configure at least one nonroot user directly on each device, in case access to the remote authentication server is disrupted. This one nonroot user commonly has a generic name, such as admin.

Because user accounts are configured on multiple devices, they are commonly configured inside of a configuration group. As such, the examples shown here are in a configuration group called global. Using a configuration group for your user accounts is optional.

To create a user account:

1. Add a new user, using the user’s assigned account login name.

```
[edit groups global]
user@host# edit system login user username
```

2. (Optional) Configure a full descriptive name for the account.

   If the full name includes spaces, enclose the entire name in quotation marks.

```
[edit groups global system login user user-name]
user@host# set full-name complete-name
```

For example:

```
user@host# show groups
global {
    system {
        login {
            user admin {
                full-name "general administrator";
            }
        }
    }
}
```

3. (Optional) Set the user identifier (UID) for the account.
As with UNIX systems, the UID enforces user permissions and file access. If you do not set the UID, Junos OS assigns one for you. The format of the UID is a number in the range of 100 to 64000.

```
[edit groups global system login user user-name]
user@host# set uid uid-value
```

For example:

```
user@host# show groups
global {
    system {
        login {
            user admin {
                uid 9999;
            }
        }
    }
}
```

4. Assign the user to a login class.

You can define your own login classes or assign one of the predefined Junos OS login classes.

The predefined login classes are as follows:

- **super-user**—all permissions
- **operator**—clear, network, reset, trace, and view permissions
- **read-only**—view permissions
- **unauthorized**—no permissions

```
[edit groups global system login user user-name]
user@host# set class class-name
```

For example:

```
user@host# show groups
global {
    system {
        login {
            user admin {
                class super-user;
            }
        }
    }
```
5. Use one of the following methods to configure the user password.

- To enter a clear-text password that the system encrypts for you, use the following command to set the user password:

  ```
  [edit groups global system login user user-name]
  user@host# set authentication plain-text-password password
  New Password: type password here
  Retype new password: retype password here
  ```

  As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are therefore hidden and marked as ## SECRET-DATA in the configuration.

- To enter a password that is already encrypted, use the following command to set the user password:

  ```
  CAUTION: Do not use the encrypted-password option unless the password is already encrypted, and you are entering the encrypted version of the password.

  If you accidentally configure the encrypted-password option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as this user.
  ```

  ```
  [edit groups global system login user user-name]
  user@host# set authentication encrypted-password "password"
  New Password: type password here
  Retype new password: retype password here
  ```

- To load previously generated public keys from a named file at a specified URL location, use the following command to set the user password:

  ```
  [edit groups global system login user user-name]
  user@host# set authentication load-key-file URL filename
  ```

- To enter an ssh public string, use the following command to set the user password:
6. At the top level of the configuration, apply the configuration group.
   If you use a configuration group, you must apply it for it to take effect.

   ```
   [edit]
   user@host# set apply-groups global
   ```

7. Commit the configuration.

   ```
   user@host# commit
   ```

8. To verify the configuration, log out and log back in as the new user.

RELATED DOCUMENTATION

- Junos OS Administrative Roles | 105
- Junos OS User Access Privileges | 117
- Junos OS User Accounts Overview | 91

Junos OS Administrative Roles

IN THIS SECTION

- Understanding Administrative Roles | 106
- Example: Configuring Administrative Roles | 108
- Configuring a Local Administrator Account | 117

Junos OS allows you to define a system user to act as a particular kind of administrator for the system. You can assign an administrative role to a user by configuring a login class to have the administrative role.
attributes. You can assign one of the role attributes such as audit-officer crypto-officer, security-officer, ids-officer to an administrative user. Read this topic for more information.

Understanding Administrative Roles

A system user can be a member of a class that allows the user to act as a particular kind of administrator for the system. Requiring a specific role to view or modify an item restricts the extent of information a user can obtain from the system. It also limits how much of the system is open to intentional or unintentional modification or observation by a user. We recommend that you use the following guidelines when you are designing administrative roles:

- Do not allow any user to log in to the system as root.
- Restrict each user to the smallest set of privileges needed to perform the user’s duties.
- Do not allow any user to belong to a login class containing the shell permission flag. The shell permission flag allows users to run the start shell command from the CLI.
- Allow users to have rollback permissions. Rollback permissions allow users to undo an action performed by an administrator but does not allow them to commit the changes.

You can assign an administrative role to a user by configuring a login class to have the privileges required for that role. You can configure each class to allow or deny access to configuration statements and commands by name. These specific restrictions override and take precedence over any permission flags also configured in the class. You can assign one of the following role attributes to an administrative user.

- **Crypto-administrator**—Allows the user to configure and monitor cryptographic data.
- **Security-administrator**—Allows the user to configure and monitor security data.
- **Audit-administrator**—Allows the user to configure and monitor audit data.
- **IDS-administrator**—Allows the user to monitor and clear the intrusion detection service (IDS) security logs.

Each role can perform the following specific management functions:

- **Cryptographic Administrator**
  - Configures the cryptographic self-test.
  - Modifies the cryptographic security data parameters.

- **Audit Administrator**
  - Configures and deletes the audit review search and sort feature.
  - Searches and sorts audit records.
• Configures search and sort parameters.
• Manually deletes audit logs.

**Security Administrator**

• Invokes, determines, and modifies the cryptographic self-test behavior.
• Enables, disables, determines, and modifies the audit analysis and audit selection functions and configures the device to automatically delete audit logs.
• Enables or disables security alarms.
• Specifies limits for quotas on Transport Layer connections.
• Specifies the limits, network identifiers, and time periods for quotas on controlled connection-oriented resources.
• Specifies the network addresses permitted to use Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP).
• Configures the time and date used in time stamps.
• Queries, modifies, deletes, and creates the information flow or access control rules and attributes for the unauthenticated information flow security function policy (SFP), the authenticated information flow SFP, the unauthenticated device services, and the discretionary access control policy.
• Specifies initial values that override default values when object information is created under unauthenticated information flow SFP, the authenticated information flow SFP, the unauthenticated target of evaluation (TOE) services, and the discretionary access control policy.
• Creates, deletes, or modifies the rules that control the address from which management sessions can be established.
• Specifies and revokes security attributes associated with the users, subjects, and objects.
• Specifies the percentage of audit storage capacity at which the device alerts administrators.
• Handles authentication failures and modifies the number of failed authentication attempts through SSH or from the CLI that can occur before progressive throttling is enforced for further authentication attempts and before the connection is dropped.
• Manages basic network configuration of the device.

**IDS Administrator**—Specifies IDS security alarms, intrusion alarms, audit selections, and audit data.

You need to set the security-role attribute in the classes created for these administrative roles. This attribute restricts which users can show and clear the security logs, actions that cannot be performed through configuration alone.

For example, you need to set the security-role attribute in the `ids-admin` class created for the IDS administrator role if you want to restrict clearing and showing IDS logs to the IDS administrator role.
Likewise, you need to set the security-role to one of the other admin values to restrict that class from being able to clear and show non-IDS logs only.

**NOTE:** When a user deletes an existing configuration, the configuration statements under the hierarchy level of the deleted configuration (that is, the child objects that the user does not have permission to modify), now remain in the device.

---

### Example: Configuring Administrative Roles

**IN THIS SECTION**

- Requirements | 108
- Overview | 108
- Configuration | 109
- Verification | 115

This example shows how to configure individual administrative roles for a distinct, unique set of privileges apart from all other administrative roles.

**Requirements**

No special configuration beyond device initialization is required before configuring this feature.

**Overview**

This example configures four users:

- **audit-officer** of the class **audit-admin**
- **crypto-officer** of the class **crypto-admin**
- **security-officer** of the class **security-admin**
- **ids-officer** of the class **ids-admin**
When a `security-admin` class is configured, the privileges for creating administrators are revoked from the user who created the `security-admin` class. Creation of new users and logins is at the discretion of the `security-officer`.

In this example, you create audit admin, crypto admin, security admin, and ids admin with permission flags pertaining to this role. Then you allow or deny access to configuration statements and commands by name for each administrative role. These specific restrictions take precedence over the permission flags also configured in the class. For example, only the `crypto-admin` can run the `request system set-encryption-key` command, which requires having the `security` permission flag to access it. Only the `security-admin` can include the `system time-zone` statement in the configuration, which requires having the `system-control` permission flag.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set system login class audit-admin permissions security
set system login class audit-admin permissions trace
set system login class audit-admin permissions maintenance
set system login class audit-admin allow-commands "^clear {log|security log}"
set system login class audit-admin deny-commands "^clear {security alarms|system login lockout}|^file (copy|delete|rename)|^request {security|system set-encryption-key}|^rollback|^set date|^show security {alarms|dynamic-policies|match-policies|policies}|^start shell";
set system login class audit-admin security-role audit-administrator
set system login class crypto-admin permissions admin-control
set system login class crypto-admin permissions configure
set system login class crypto-admin permissions maintenance
set system login class crypto-admin permissions security-control
set system login class crypto-admin permissions system-control
set system login class crypto-admin permissions trace
set system login class crypto-admin allow-commands "^request system set-encryption-key"
set system login class crypto-admin deny-commands "^clear {log|security alarms|security log|system login lockout}|^file (copy|delete|rename)|^rollback|^set date|^show security {alarms|dynamic-policies|match-policies|policies}|^start shell";
set system login class crypto-admin allow-configuration-regexps "security {ike|ipsec} {policy|proposal}" "security ipsec ^vpn$" "^manual {authentication|encryption|protocol|spi}" "system fips self-test after-key-generation"
set system login class crypto-admin security-role crypto-administrator
set system login class security-admin permissions all
set system login class security-admin deny-commands "^clear {log|security log}|^clear|show security alarms alarm-type idp|^request {security|system set-encryption-key}|^rollback|^start shell"
```
set system login class security-admin deny-configuration-regexps "security alarms potential-violation idp" "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$.* manual (authentication|encryption|protocol|spi)" "security log cache" "security log exclude .* event-id IDP_.*" "system fips self-test after-key-generation" set system login class security-admin security-role security-administrator set system login class ids-admin permissions configure set system login class ids-admin permissions security-control set system login class ids-admin permissions trace set system login class ids-admin permissions maintenance set system login class ids-admin allow-configuration-regexps "security alarms potential-violation idp" "security log exclude .* event-id IDP_.*" set system login class ids-admin deny-commands "^clear log!\(clear\show\) security alarms (alarm-id\(all\ newer-than\ older-than\ process\severity\)\(clear\show\) security alarms alarm-type (authentication|cryptographic-self-test|decryption-failures|encryption-failures) ike-phase1-failures ike-phase2-failures key-generation-self-test) non-cryptographic-self-test\(policy\replay-attacks\)\(file\copy\delete\rename\)\(request\(security\system set-encryption-key\)\(rollback\)\(set date\)\(show\(dynamic-policies\match-policies\policies\)\(start shell\) set system login class ids-admin deny-configuration-regexps "security alarms potential-violation (authentication|cryptographic-self-test|decryption-failures|encryption-failures)ike-phase1-failuresike-phase2-failureskey-generation-self-testnon-cryptographic-self-test\(policy\\(replay-attacks\)\(file\copy\delete\rename\)\(request\(security\system set-encryption-key\)\(rollback\)\(set date\)\(show\(dynamic-policies\match-policies\policies\)\(start shell\) set system login user audit-officer class audit-admin set system login user crypto-officer class crypto-admin set system login user security-officer class security-admin set system login user ids-officer class ids-admin set system login user audit-officer authentication plain-text-password set system login user crypto-officer authentication plain-text-password set system login user security-officer authentication plain-text-password set system login user ids-officer authentication plain-text-password

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure users in administrative roles:

1. Create the **audit-admin** login class.

   ```
   [edit]
   user@host# set system login class audit-admin
   [edit system login class audit-admin]
   user@host# set permissions security
   user@host# set permissions trace
   ```
2. Configure the **audit-admin** login class restrictions.

   ```
   [edit system login class audit-admin]
   user@host# set allow-commands "^clear (log|security log)"
   user@host# set deny-commands "^clear (security alarms|system login lockout)|^file
   (copy|delete|rename)|^request (security|system set-encryption-key)|^rollback|^set date|^show security
   (alarms|dynamic-policies|match-policies|policies)|^start shell"
   user@host# set security-role audit-administrator
   ```

3. Create the **crypto-admin** login class.

   ```
   [edit]
   user@host# set system login class crypto-admin
   [edit system login class crypto-admin]
   user@host# set permissions admin-control
   user@host# set permissions configure
   user@host# set permissions maintenance
   user@host# set permissions security-control
   user@host# set permissions system-control
   user@host# set permissions trace
   ```

4. Configure the **crypto-admin** login class restrictions.

   ```
   [edit system login class crypto-admin]
   user@host# set allow-commands "^request system set-encryption-key"
   user@host# set deny-commands "^clear (log|security alarms|security log|system login lockout)|^file
   (copy|delete|rename)|^rollback|^set date|^show security
   (alarms|dynamic-policies|match-policies|policies)|^start shell"
   user@host# set allow-configuration-regexp "security (ike|ipsec) (policy|proposal)" "security ipsec ^vpn$ .*
   manual (authentication|encryption|protocol|spi)" "system fips self-test after-key-generation"
   user@host# set security-role crypto-administrator
   ```

5. Create the **security-admin** login class.

   ```
   [edit]
   user@host# set system login class security-admin
   ```
6. Configure the **security-admin** login class restrictions.

```plaintext
[edit system login class security-admin]
user@host# set permissions all
```

```plaintext
[edit system login class security-admin]
user@host# set deny-commands "^clear \(log|security log\)\|^\(clear|show\) security alarms alarm-type idp\|^request \(security\|system\|set-encryption-key\)\|^rollback\|^start shell"
user@host# set deny-configuration-regexps "security alarms potential-violation idp" "security (ike|ipsec) \(policy\|proposal\)" "security ipsec \^\(vpn\|.*\) manual \(authentication\|encryption\|protocol\|spi\)" "security log cache" "security log exclude .* event-id IDP_.*" "system fips self-test after-key- generation"
```

7. Create the **ids-admin** login class.

```plaintext
[edit]
user@host# set system login class ids-admin
```

```plaintext
[edit system login class ids-admin]
user@host# set permissions configure
user@host# set permissions maintenance
user@host# set permissions security-control
user@host# set permissions trace
```

8. Configure the **ids-admin** login class restrictions.

```plaintext
[edit system login class ids-admin]
user@host# set allow-configuration-regexps "security alarms potential-violation idp" "security log exclude .* event-id IDP_.*"
```

```plaintext
set system login class ids-admin deny-commands "^clear \(log\|security log\)\|^\(clear|show\) security alarms\(^\(alarm-id\|all\|newer\-than\|older\-than\|process\|severity\)\|^\(clear|show\) security alarms alarm-type\(authentication\|cryptographic\-self-\test\|decryption-\failures\|encryption-\failures\)\|ike\-phase1\-failures\|ike\-phase2\-failures\|key\-generation\-self\-test\)\|\^\(rollback\|\^date\)\|\^show security \(dynamic\-policies\|match\-policies\|policies\)\|^start shell"
```

```plaintext
set system login class ids-admin deny-configuration-regexps "security alarms potential-violation \(authentication\|cryptographic\-self-\test\|decryption-\failures\|encryption-\failures\)\|ike\-phase1\-failures\|ike\-phase2\-failures\|key\-generation\-self-\test\)\|\^\(rollback\|\^date\)\|^\(clear\|delete\|rename\)\|^request \(security\|system\)\|\(set-encryption-key\)\]
```
9. Assign users to the roles.

```
[edit]
user@host# set system login

[edit system login]
user@host# set user audit-officer class audit-admin
user@host# set user crypto-officer class crypto-admin
user@host# set user security-officer class security-admin
user@host# set user ids-officer class ids-admin
```

10. Configure passwords for the users.

```
[edit system login]
user@host# set user audit-officer authentication plain-text-password
user@host# set user crypto-officer authentication plain-text-password
user@host# set user security-officer authentication plain-text-password
user@host# set user ids-officer authentication plain-text-password
```

**Results**

From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show system
system {
  login {
    class audit-admin {
      permissions [ maintenance security trace ];
      allow-commands "^clear (log|security log)";
      deny-commands "^clear (security alarms|system login lockout)|^file (copy|delete|rename)|^request (security|system set-encryption-key)|^rollback|^setdate|^show security (alarms|dynamic-policies|match-policies|policies)|^start shell";
      security-role audit-administrator;
    }
    class crypto-admin {
      permissions [ admin-control configure maintenance security-control system-control trace ];
      allow-commands "^request (system set-encryption-key)";
    }
  }
```
deny-commands "^clear (log|security alarms|security log)system login lockout|\^file (copy|delete|rename)\^rollback\^set date|\^show security (alarms|dynamic-policies|match-policies|policies)__\^start shell";
allow-configuration-regexps "security (ike|ipsec) (policy|proposal)" __"security ipsec \^vpn\$." __manual (authentication|encryption|protocol|spi)__ "system fips self-test after-key-generation";
security-role crypto-administrator;
}
class security-admin {
permissions [all];
deny-commands __"^clear (log|security log)|\^clear|\^show security alarms alarm-type idp|\^request (security|system set-encryption-key)\^rollback\^start shell";
deny-configuration-regexps __"security alarms potential-violation idp" __"security (ike|ipsec) (policy|proposal)" __"security ipsec \^vpn\$." __manual (authentication|encryption|protocol|spi)__ __"security log exclude ." __event-id IDP__\^-" __"system fips self-test after-key-generation";
security-role security-administrator;
}
class ids-admin {
permissions [ configure maintenance security-control trace ];
deny-commands __"^clear log|\^clear|\^show security alarms alarm-type (alarm-id|all|newer-than|older-than|process|severity)|\^clear|\^show security alarms alarm-type (authentication | cryptographic-self-test | decryption-failures | encryption-failures | ike-phase1-failures | ike-phase2-failures|key-generation-self-test | non-cryptographic-self-test | policy | replay-attacks) | ^file (copy|delete|rename) | ^=request (security|system set-encryption-key) | ^=rollback | ^=set date | ^=show security (dynamic-policies|match-policies|policies) | ^=start shell";
allow-configuration-regexps __"security alarms potential-violation idp" __"security log exclude ." __event-id IDP__^-" __; 
}
user audit-officer {
  class audit-admin;
  authentication {
    encrypted-password "$1$ABC123"; ## SECRET-DATA
  }
}
user crypto-officer {
  class crypto-admin;
  authentication {
    encrypted-password "$1$ABC123."; ## SECRET-DATA
  }
}
If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

Confirm that the configuration is working properly.

**Verifying the Login Permissions**

**Purpose**

Verify the login permissions for the current user.

**Action**

From operational mode, enter the `show cli authorization` command.

```
user@host> show cli authorization
```

Current user: 'example' class 'super-user'

Permissions:

- admin      -- Can view user accounts
- admin-control -- Can modify user accounts
- clear      -- Can clear learned network info
- configure  -- Can enter configuration mode
- control    -- Can modify any config
- edit       -- Can edit full files
- field      -- Can use field debug commands
- floppy     -- Can read and write the floppy
- interface  -- Can view interface configuration
- interface-control -- Can modify interface configuration
network     -- Can access the network
reset       -- Can reset/restart interfaces and daemons
routing     -- Can view routing configuration
routing-control -- Can modify routing configuration
shell       -- Can start a local shell
snmp        -- Can view SNMP configuration
snmp-control-- Can modify SNMP configuration
system      -- Can view system configuration
system-control-- Can modify system configuration
trace       -- Can view trace file settings
trace-control-- Can modify trace file settings
view        -- Can view current values and statistics
maintenance -- Can become the super-user
firewall     -- Can view firewall configuration
firewall-control-- Can modify firewall configuration
secret      -- Can view secret statements
secret-control-- Can modify secret statements
rollback    -- Can rollback to previous configurations
security     -- Can view security configuration
security-control-- Can modify security configuration
access      -- Can view access configuration
access-control-- Can modify access configuration
view-configuration-- Can view all configuration (not including secrets)
flow-tap     -- Can view flow-tap configuration
flow-tap-control-- Can modify flow-tap configuration
idp-profiler-operation-- Can Profiler data
pgcp-session-mirroring-- Can view pgcp session mirroring configuration
pgcp-session-mirroring-control-- Can modify pgcp session mirroring configuration
storage     -- Can view fibre channel storage protocol configuration
storage-control-- Can modify fibre channel storage protocol configuration
all-control -- Can modify any configuration

Individual command authorization:
Allow regular expression: none
Deny regular expression: none
Allow configuration regular expression: none
Deny configuration regular expression: none

This output summarizes the login permissions.
Configuring a Local Administrator Account

The following example shows how to configure a password-protected local administration account called admin with superuser privileges. Superuser privileges give a user permission to use any command on the router and are generally reserved for a select few users such as system administrators. It is important to protect the local administrator account with a password to prevent unauthorized users from gaining access to superuser commands that can be used to alter the system configuration. Even users with RADIUS authentication should configure a local password. If RADIUS fails or becomes unreachable, the login process will revert to password authentication on the local administrator account.

```
[edit]
  system {
    login {
      user admin {
        uid 1000;
        class superuser;
        authentication {
          encrypted-password "<PASSWORD>"; # SECRET-DATA
        }
      }
    }
  }
```

RELATED DOCUMENTATION

- Junos OS Login Classes Overview | 69
- Configuring Junos OS User Accounts by Using a Configuration Group | 102

Junos OS User Access Privileges

IN THIS SECTION

- Understanding Junos OS Access Privilege Levels | 118
- Example: Configuring User Permissions with Access Privilege Levels | 124
- Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies | 128
Junos OS allows you to grant the access or permissions to the commands and configuration hierarchy levels and statements. This enables users to execute only those commands and configure and view only those statements for which they have access privileges. You can use extended regular expressions to specify which operational mode commands, configuration statements, and hierarchies are denied or allowed for users. This prevents unauthorized users from executing or configuring sensitive commands and statements that could potentially cause damage to the network. Read this topic for more information.

Understanding Junos OS Access Privilege Levels

Each top-level CLI command and each configuration statement have an access privilege level associated with them. Users can execute only those commands and configure and view only those statements for which they have access privileges. The access privileges for each login class are defined by one or more permission flags.

For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the permissions statement.

The following sections provide additional information about permissions:
Junos OS Login Class Permission Flags

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user's login class at the [edit system login class] hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the all permissions flag.

**NOTE:** Each command listed represents that command and all subcommands with that command as a prefix. Each configuration statement listed represents the top of the configuration hierarchy to which that flag grants access.

The permissions statement specifies one or more of the permission flags listed in Table 5 on page 119. Permission flags are not cumulative, so for each class you must list all the permission flags needed, including view to display information and configure to enter configuration mode. Two forms of permissions control for individual parts of the configuration are:

- "Plain" form—Provides read-only capability for that permission type. An example is interface.
- Form that ends in -control—Provides read and write capability for that permission type. An example is interface-control.

For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the interface permissions flag grants read-only access to the [edit interfaces] hierarchy level. The -control form of the flag grants read-write access to that configuration. Using the preceding example, interface-control grants read-write access to the [edit interfaces] hierarchy level.

Table 5 on page 119 lists the Junos OS login class permission flags that you can configure by including the permissions statement at the [edit system login class class-name] hierarchy level.

The permission flags grant a specific set of access privileges. Each permission flag is listed with the operational mode commands and configuration hierarchy levels and statements for which that flag grants access.

Table 5: Login Class Permission Flags

<table>
<thead>
<tr>
<th>Permission Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;access&quot; on page 1035</td>
<td>Can view the access configuration in configuration mode and with the show configuration operational mode command.</td>
</tr>
<tr>
<td>&quot;access-control&quot; on page 1040</td>
<td>Can view and configure access information at the [edit access] hierarchy level.</td>
</tr>
<tr>
<td>Permission Flag</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>“admin” on page 1041</td>
<td>Can view user account information in configuration mode and with the show configuration operational mode command.</td>
</tr>
<tr>
<td>“admin-control” on page 1047</td>
<td>Can view user account information and configure it at the [edit system] hierarchy level.</td>
</tr>
<tr>
<td>“all-control” on page 1048</td>
<td>Can view user accounts and configure them at the [edit system login] hierarchy level.</td>
</tr>
<tr>
<td>all</td>
<td>Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.</td>
</tr>
<tr>
<td>“clear” on page 1049</td>
<td>Can clear (delete) information learned from the network that is stored in various network databases by using the clear commands.</td>
</tr>
<tr>
<td>“configure” on page 1150</td>
<td>Can enter configuration mode by using the configure command.</td>
</tr>
<tr>
<td>“control” on page 1151</td>
<td>Can perform all control-level operations—all operations configured with the -control permission flags.</td>
</tr>
<tr>
<td>“field” on page 1152</td>
<td>Can view field debug commands. Reserved for debugging support.</td>
</tr>
<tr>
<td>“firewall” on page 1153</td>
<td>Can view the firewall filter configuration in configuration mode.</td>
</tr>
<tr>
<td>“firewall-control” on page 1159</td>
<td>Can view and configure firewall filter information at the [edit firewall] hierarchy level.</td>
</tr>
<tr>
<td>“floppy” on page 1160</td>
<td>Can read from and write to the removable media.</td>
</tr>
<tr>
<td>“flow-tap” on page 1161</td>
<td>Can view the flow-tap configuration in configuration mode.</td>
</tr>
<tr>
<td>“flow-tap-control” on page 1165</td>
<td>Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap] hierarchy level.</td>
</tr>
<tr>
<td>“flow-tap-operation” on page 1166</td>
<td>Can make flow-tap requests to the router or switch. For example, a Dynamic Tasking Control Protocol (DTCP) client must have flow-tap-operation permission to authenticate itself to the Junos OS as an administrative user.</td>
</tr>
</tbody>
</table>

**NOTE:** The flow-tap-operation option is not included in the all-control permissions flag.
<table>
<thead>
<tr>
<th>Permission Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;idp-profiler-operation&quot; on page 1167</td>
<td>Can view profiler data.</td>
</tr>
<tr>
<td>&quot;interface&quot; on page 1168</td>
<td>Can view the interface configuration in configuration mode and with the <code>show configuration</code> operational mode command.</td>
</tr>
</tbody>
</table>
| "interface-control" on page 1173 | Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the following hierarchy levels:  
  - [edit chassis]  
  - [edit class-of-service]  
  - [edit groups]  
  - [edit forwarding-options]  
  - [edit interfaces] |
| "maintenance" on page 1175 | Can perform system maintenance, including starting a local shell on the router or switch and becoming the superuser in the shell by using the `su root` command, and can halt and reboot the router or switch by using the `request system` commands. |
| "network" on page 1187 | Can access the network by using the `ping`, `ssh`, `telnet`, and `traceroute` commands. |
| "pgcp-session-mirroring" on page 1190 | Can view the `pgcp` session mirroring configuration. |
| "pgcp-session-mirroring-control" on page 1195 | Can modify the `pgcp` session mirroring configuration. |
| "reset" on page 1196 | Can restart software processes by using the `restart` command and can configure whether software processes are enabled or disabled at the [edit system processes] hierarchy level. |
| "rollback" on page 1197 | Can use the `rollback` command to return to a previously committed configuration other than the most recently committed one. |
| "routing" on page 1198 | Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes. |
### Table 5: Login Class Permission Flags (continued)

<table>
<thead>
<tr>
<th>Permission Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;routing-control&quot; on page 1209</td>
<td>Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level.</td>
</tr>
<tr>
<td>&quot;secret&quot; on page 1215</td>
<td>Can view passwords and other authentication keys in the configuration.</td>
</tr>
<tr>
<td>&quot;secret-control&quot; on page 1221</td>
<td>Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.</td>
</tr>
<tr>
<td>&quot;security&quot; on page 1223</td>
<td>Can view security configuration in configuration mode and with the show configuration operational mode command.</td>
</tr>
<tr>
<td>&quot;security-control&quot; on page 1233</td>
<td>Can view and configure security information at the [edit security] hierarchy level.</td>
</tr>
<tr>
<td>&quot;shell&quot; on page 1238</td>
<td>Can start a local shell on the router or switch by using the start shell command.</td>
</tr>
<tr>
<td>&quot;snmp&quot; on page 1239</td>
<td>Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.</td>
</tr>
<tr>
<td>&quot;snmp-control&quot; on page 1243</td>
<td>Can view SNMP configuration information and can modify SNMP configuration at the [edit snmp] hierarchy level.</td>
</tr>
<tr>
<td>&quot;system&quot; on page 1244</td>
<td>Can view system-level information in configuration and operational modes.</td>
</tr>
<tr>
<td>&quot;system-control&quot; on page 1252</td>
<td>Can view system-level configuration information and configure it at the [edit system] hierarchy level.</td>
</tr>
<tr>
<td>&quot;trace&quot; on page 1255</td>
<td>Can view trace file settings and configure trace file properties.</td>
</tr>
<tr>
<td>&quot;trace-control&quot; on page 1266</td>
<td>Can modify trace file settings and configure trace file properties.</td>
</tr>
<tr>
<td>&quot;view&quot; on page 1274</td>
<td>Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.</td>
</tr>
<tr>
<td>&quot;view-configuration&quot; on page 1423</td>
<td>Can view all of the configuration excluding secrets, system scripts, and event options.</td>
</tr>
</tbody>
</table>

**NOTE:** Only users with the maintenance permission can view commit script, op script, or event script configuration.
Allowing or Denying Individual Commands for Junos OS Login Classes

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level specified in the permissions statement.

Permission flags are used to grant a user access to operational mode commands and configuration hierarchy levels and statements. By specifying a specific permission flag on the user’s login class at the [edit system login class] hierarchy level, you grant the user access to the corresponding commands and configuration hierarchy levels and statements. To grant access to all commands and configuration statements, use the all permissions flag. For permission flags that grant access to configuration hierarchy levels and statements, the flags grant read-only privilege to that configuration. For example, the interface permissions flag grants read-only access to the [edit interfaces] hierarchy level. The -control form of the flag grants read-write access to that configuration. Using the preceding example, interface-control grants read-write access to the [edit interfaces] hierarchy level.

- The all login class permission bits take precedence over extended regular expressions when a user issues rollback command with rollback permission flag enabled.
- Expressions used to allow and deny commands for users on RADIUS and TACACS+ servers have been simplified. Instead of a single, long expression with multiple commands (allow-commands=cmd1 cmd2 ... cmdn), you can specify each command as a separate expression. This new syntax is valid for allow-configuration, deny-configuration, allow-commands, deny-commands, and all user permission bits.
- Users cannot issue the load override command when specifying an extended regular expression. Users can only issue the merge, replace, and patch configuration commands.
- If you allow and deny the same commands, the allow-commands permissions take precedence over the permissions specified by the deny-commands. For example, if you include allow-commands "request system software add" and deny-commands "request system software add", the login class user is allowed to install software using the request system software add command.
- Regular expressions for allow-commands and deny-commands can also include the commit, load, rollback, save, status, and update commands.
- If you specify a regular expression for allow-commands and deny-commands with two different variants of a command, the longest match is always executed.

For example, if you specify a regular expression for allow-commands with the commit-synchronize command and a regular expression for deny-commands with the commit command, users assigned to such a login class would be able to issue the commit synchronize command, but not the commit command. This is because commit-synchronize is the longest match between commit and commit-synchronize and it is specified for allow-commands.

Likewise, if you specify a regular expression for allow-commands with the commit command and a regular expression for deny-commands with the commit-synchronize command, users assigned to such
a login class would be able to issue the `commit` command, but not the `commit-synchronize` command. This is because `commit-synchronize` is the longest match between `commit` and `commit-synchronize` and it is specified for `deny-commands`.

### Example: Configuring User Permissions with Access Privilege Levels

This example shows how to view permissions for a user account and configure the user permissions with access privileges for a login class. This enables users to execute only those commands and configure and view only those statements for which they have access privileges. This prevents unauthorized users from executing or configuring sensitive commands and statements that could potentially cause damage to the network.

#### Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish connection between the device and the TACACS+ server.

  For information on configuring a TACACS+ server, see “Configuring TACACS+ Authentication” on page 264.

- Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.
Overview

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the permissions statement at the [edit system login class class-name] hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the permissions statement. Permission flags are used to grant a user access to operational mode commands, statements, and configuration hierarchies. Permission flags are not cumulative, so for each login class you must list all the permission flags needed, including view to display information and configure to enter configuration mode. By specifying a specific permission flag on the user's login class, you grant the user access to the corresponding commands, statements, and configuration hierarchies. To grant access to all commands and configuration statements, use the all permissions flag. The permission flags provide read-only (“plain” form) and read and write (form that ends in -control) capability for a permission type.

NOTE: The all login class permission bits take precedence over extended regular expressions when a user issues a rollback command with the rollback permission flag enabled.

To configure user access privilege levels:

1. View permissions for a user account.

You can view the permissions for a user account before configuring the access privileges for those permissions.

To view the user permissions, enter ? at the [edit] hierarchy level:

```
[edit]
?
```

2. Configure user permissions with access privileges.

All users who can log in to a device must be in a login class. For each login class, you can configure the access privileges that the associated users can have when they are logged in to the device.

To configure access privilege levels for user permissions, include the permissions statement at the [edit system login class class-name] hierarchy level, followed by the user permission, the permissions option, and the required permission flags.

```
[edit system login]
```
Configuration

Configuring User Permissions with Access Privilege Levels

Step-by-Step Procedure
To configure access privileges:

1. From the device, view the list of permissions available for the user account. In this example, the username of the user account is host.

```
[edit]
user@host> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  load                 Load information from file
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  save                 Save information to file
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

The output lists the permissions for the user host. Customized login classes can be created by configuring different access privileges on these user permissions.

2. Configure an access privilege class to enable user host to configure and view SNMP parameters only. In this example, this login class is called network-management. To customize the network-management login class, include the SNMP permission flags to the `configure` user permission.
Here, the configured permission flags provide both read (snmp) and read-and-write (snmp-control) capability for SNMP, and this is the only allowed access privilege for the network-management login class. In other words, all other access privileges other than configuring and viewing SNMP parameters are denied.

**Results**

From configuration mode, confirm your configuration by entering the `show system login` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show system login
class network-management {
    permissions [ configure snmp snmp-control ];
}
```

**Verification**

Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

**Verifying SNMP Configuration**

**Purpose**

Verify that SNMP configuration can be executed.

**Action**
From configuration mode, execute basic SNMP commands at the [edit snmp] hierarchy level.

```
[edit snmp]
user@host# set name device1
user@host# set description switch1
user@host# set location Lab1
user@host# set contact example.com
user@host# commit
```

**Meaning**
The user host assigned to the network-management login class is able to configure SNMP parameters, as the permission flags specified for this class include both snmp (read capabilities) and snmp-control (read and write capabilities) permission bits.

**Verifying non-SNMP Configuration**

**Purpose**
Verify that non-SNMP configuration is denied for the network-management login class.

**Action**
From the configuration mode, execute any non-SNMP configuration, for example, interfaces configuration.

```
[edit]
user@host# edit interfaces
Syntax error, expecting <statement> or <identifier>.
```

**Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies**

**IN THIS SECTION**

- Understanding Regular Expressions  | 129
- Specifying Regular Expressions  | 131
- Regular Expressions Operators  | 133
- Regular Expression Examples  | 136
This topic contains the following sections:

**Understanding Regular Expressions**

You can use extended regular expressions to specify which operational mode commands, configuration statements, and hierarchies are denied or allowed. You specify these regular expressions locally in the `allow/deny-commands`, `allow/deny-configuration`, and `allow/deny-commands-regexps` and `allow/deny-configuration-regexp` statements at the `[edit system login class class-name]` hierarchy level, or remotely by specifying Juniper Networks vendor-specific TACACS+ or RADIUS attributes in your authorization server's configuration.

NOTE: Starting in Junos OS Release 18.1, the `allow-commands-regexps` and `deny-commands-regexps` statements are supported for TACACS+ authorization.

The difference between a local and remote authorization configuration is the pattern in which the regular expressions statements are executed. While it is possible to specify multiple regular expressions using strings in the local authorization configuration, in a remote configuration, the regular expressions statements need to be split and specified in individual strings. When the authorization parameters are configured both remotely and locally, the regular expressions received during TACACS+ or RADIUS authorization get merged with any regular expressions available on the local device.

When specifying multiple regular expressions in a local configuration using the `allow-configuration`, `deny-configuration`, `allow-commands`, or `deny-commands` statements, regular expressions are configured within parentheses and separated using the pipe symbol. The complete expression is enclosed in double quotes. For example, you can specify multiple `allow-commands` parameters with the following syntax:

```
allow-commands "(cmd1)|(cmd2)|(cmdn)"
```

The same expression configured remotely on the authorization server uses the following syntax:

```
allow-commands1 = "cmd1"
allow-commands2 = "cmd2"
allow-commandsn = "cmdn"
```

When specifying multiple regular expressions in a local configuration using the `allow-configuration-regexps`, `deny-configuration-regexps`, `allow-commands-regexps`, or `deny-commands-regexps` statements, regular expressions are configured within double quotes and separated using the space operator. The complete expression is enclosed in square brackets. For example, you can specify multiple `allow-commands` parameters with the following syntax:
allow-commands-regexps [ "cmd1" "cmd2" "cmdn" ]

The same expression configured remotely on the authorization server uses the following syntax:

allow-commands-regexps1 = "cmd1"
allow-commands-regexps2 = "cmd2"
allow-commands-regexpsn = "cmdn"

Table 6 on page 130 differentiates the local and remote authorization configuration using regular expressions.

<table>
<thead>
<tr>
<th>Local Configuration</th>
<th>Remote Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>login {</td>
<td>user = remote {</td>
</tr>
<tr>
<td>class local {</td>
<td>login = username</td>
</tr>
<tr>
<td>permissions configure;</td>
<td>service = junos-exec {</td>
</tr>
<tr>
<td>allow-commands &quot;(ping .<em>)(traceroute .</em>)</td>
<td>(show .*)</td>
</tr>
<tr>
<td>deny-commands .*;</td>
<td>allow-commands2 = &quot;traceroute .*&quot;</td>
</tr>
<tr>
<td>allow-configuration &quot;(interfaces .* unit 0 family ethernet-switching vlan mem.* .*)</td>
<td>(interfaces .* native.* .*)</td>
</tr>
<tr>
<td>deny-configuration .*;</td>
<td>deny-commands4 = &quot;configure&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands5 = &quot;edit&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands6 = &quot;exit&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands7 = &quot;commit&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands8 = &quot;,xml-mode&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands9 = &quot;,netconf&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands10 = &quot;,need-trailer&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-commands11 = &quot;rollback.&quot;</td>
</tr>
<tr>
<td></td>
<td>deny-commands1 = &quot;,&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration1 = &quot;interfaces .* unit 0 family ethernet-switching vlan mem.* .*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration2 = &quot;interfaces .* native.* .*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration3 = &quot;interfaces .* unit 0 family ethernet-switching interface-mo.* .*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration4 = &quot;interfaces .* unit .*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration5 = &quot;interfaces .* disable&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration6 = &quot;interfaces .* description.*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration7 = &quot;interfaces .*&quot;</td>
</tr>
<tr>
<td></td>
<td>allow-configuration8 = &quot;vlans .* vlan-.* .*&quot;</td>
</tr>
<tr>
<td></td>
<td>deny-configuration1 = &quot;,&quot;</td>
</tr>
<tr>
<td></td>
<td>local-user-name = local-username</td>
</tr>
<tr>
<td></td>
<td>user-permissions = &quot;configure&quot;</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
</tr>
</tbody>
</table>

Table 6: Sample Local and Remote Authorization Configuration Using Regular Expressions
NOTE:

- You need to explicitly allow access to the NETCONF mode, either locally or remotely, by issuing the following three commands: `xml-mode`, `netconf`, and `need-trailer`.

- When the `deny-configuration = ".*"` statement is used, all the other desired configurations should be allowed using the `allow-configuration` statement. This can affect the allowed regular expressions buffer limit for the `allow-configuration` statement. When this limit exceeds, the allowed configuration might not work. This regular expression buffer size limit has been increased in Junos OS Release 14.1x53-D40, 15.1, and 16.1.

Specifying Regular Expressions

**WARNING:** When you specify regular expression for commands and configuration statements, pay close attention to the following examples, as regular expression with invalid syntax might not produce the desired results, even if the configuration is committed without any error.

Regular expressions for commands and configuration statements should be specified in the same manner as executing the complete command or statement. Table 7 on page 132 lists the regular expressions for configuring access privileges for the `[edit interfaces]` and `[edit vlans]` statement hierarchies, and for the `delete interfaces` command.
Table 7: Specifying Regular Expressions

<table>
<thead>
<tr>
<th>Statement</th>
<th>Regular Expression</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>[edit interfaces]</td>
<td></td>
<td>- The .* operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any interface name with any unit value.</td>
</tr>
<tr>
<td>The set command for interfaces is executed as</td>
<td></td>
<td>- Specifying only the deny-configuration &quot;interfaces.*&quot; statement is incorrect and does not deny access to the interfaces configuration for the specified login class.</td>
</tr>
<tr>
<td>follows:</td>
<td></td>
<td>- Other valid options can be included in the regular expression, for example:</td>
</tr>
<tr>
<td>[edit]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user@host# set interfaces</td>
<td></td>
<td>[edit system login class class-name]</td>
</tr>
<tr>
<td>interface-name unit</td>
<td></td>
<td>user@host# set permissions configure</td>
</tr>
<tr>
<td>interface-unit-number</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* unit .&quot;</td>
</tr>
<tr>
<td>[edit system login class class-name]</td>
<td></td>
<td>[edit system login class class-name]</td>
</tr>
<tr>
<td>user@host# set permissions configure</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* description .&quot;</td>
</tr>
<tr>
<td>user@host# set deny-configuration</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* description .&quot;</td>
</tr>
<tr>
<td>&quot;interfaces .*&quot;</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* description .&quot;</td>
</tr>
<tr>
<td>&quot;interfaces .* unit .&quot;</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* description .&quot;</td>
</tr>
<tr>
<td>&quot;interfaces .* unit . family inet address .&quot;</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* unit . family inet address .&quot;</td>
</tr>
<tr>
<td>&quot;interfaces .* disable&quot;</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .* unit . family inet address .&quot;</td>
</tr>
<tr>
<td>[edit system login class class-name]</td>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .<em>unit 0 family ethernet-switching vlan mem.</em> .&quot;</td>
</tr>
<tr>
<td>user@host# set permissions configure</td>
<td></td>
<td>Note: The mem.* regular expression in this example is used when multiple strings starting with the mem keyword are expected to be included in the specified regular expression. When only one member string is expected to be included, the member.* regular expression is used.</td>
</tr>
<tr>
<td>user@host# set allow-configuration-regexp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[edit interfaces]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The set interfaces statement is incomplete by</td>
<td></td>
<td></td>
</tr>
<tr>
<td>itself, and requires the unit option to execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the statement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>As a result, the regular expression required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for denying the set interfaces configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>must specify the entire executable string with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the .* operator in place of statement variables:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[edit system login class class-name]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user@host# set permissions configure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user@host# set deny-configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;interfaces .* unit .&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[edit system login class class-name]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user@host# set permissions configure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>user@host# set allow-configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;interfaces .* unit 0 family</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching vlan mem.* .&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: The mem.* regular expression in this</td>
<td></td>
<td></td>
</tr>
<tr>
<td>example is used when multiple strings starting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with the mem keyword are expected to be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>included in the specified regular expression.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When only one member string is expected to be</td>
<td></td>
<td></td>
</tr>
<tr>
<td>included, the member.* regular expression is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>used.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 7: Specifying Regular Expressions (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Regular Expression</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delete interfaces</code></td>
<td>The <code>delete interfaces</code> statement can be executed by itself and does not require additional statements to be complete.</td>
<td>• The <code>.*</code> operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any interface name.</td>
</tr>
<tr>
<td></td>
<td>As a result, the regular expression required for denying the <code>delete interfaces</code> statement should specify the following:</td>
<td>• For the <code>deny-configuration &quot;interfaces .*&quot;</code> regular expression to take effect, the specified login class should allow configuration permissions for the interfaces hierarchy using the <code>allow-configuration &quot;interfaces .*&quot;</code> regular expression.</td>
</tr>
<tr>
<td></td>
<td>[edit system login class class-name]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user@host# set permissions configure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user@host# set allow-configuration &quot;interfaces .*&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user@host# set deny-configuration &quot;interfaces .*&quot;</td>
<td></td>
</tr>
<tr>
<td>[edit vlans]</td>
<td>Here, the <code>set vlans</code> statement is incomplete by itself, and requires the <code>vlan-id</code> option to execute the statement.</td>
<td>• The <code>.*</code> operator denotes everything from the specified point onward for that particular command or statement. In this example, it denotes any VLAN name with any VLAN ID.</td>
</tr>
<tr>
<td></td>
<td>As a result, the regular expression required for allowing the <code>set vlans</code> configuration must specify the entire executable string with the <code>.*</code> operator in place of statement variables:</td>
<td>• Other valid options under the [edit vlans] statement hierarchy can be included in the regular expression, for example:</td>
</tr>
<tr>
<td></td>
<td>[edit system login class class-name]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user@host# set permissions configure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user@host# set allow-configuration &quot;vlans .* vlan-id .*&quot;</td>
<td></td>
</tr>
<tr>
<td>[edit vlans]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Regular Expressions Operators</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 8 on page 134** lists common regular expression operators that you can use for allowing or denying operational and configuration modes.

Command regular expressions implement the extended (modern) regular expressions, as defined in POSIX 1003.2.
### Table 8: Common Regular Expression Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Match</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>One of two or more terms separated by the pipe. Each term must be a complete standalone expression enclosed in parentheses (()), with no spaces between the pipe and the adjacent parentheses.</td>
<td>[edit system login class test] user@host# set permissions configure user@host# set allow-commands &quot;(ping)</td>
</tr>
<tr>
<td>^</td>
<td>At the beginning of an expression, used to denote where the command begins, where there might be some ambiguity.</td>
<td>[edit system login class test] user@host# set permissions interface user@host# set permissions interface-control user@host# set allow-commands &quot;(^show) (log</td>
</tr>
<tr>
<td>$</td>
<td>Character at the end of a command. Used to denote a command that must be matched exactly up to that point.</td>
<td>[edit system login class test] user@host# set permissions interface user@host# set allow-commands &quot;(show interfaces$)&quot;</td>
</tr>
</tbody>
</table>

With the above configuration, the users assigned to the test login class have operational mode access restricted to only the commands specified in the allow-commands statement, and access to the configuration mode, excluding the hierarchy levels specified in the deny-configuration statement.

With the above configuration, the users assigned to the test login class have access to configuring and viewing interface configuration from the operational and configuration mode. The allow-commands statement specifies access to commands that begin with show and monitor keywords.

For the first filter, the commands specified include the show log, show interfaces, and show policer commands. The second filter specifies all commands starting with the monitor keyword, such as monitor interfaces or monitor traffic commands.

With the above configuration, the users assigned to the test login class can view the interface configuration in the configuration mode and with the show configuration operational mode command with the interface user permission. However, the regular expression specified in the allow-commands statement restricts the users to execute only the show interfaces command and denies access to the command extensions, such as show interfaces detail or show interfaces extensive.
<table>
<thead>
<tr>
<th>Operator</th>
<th>Match</th>
<th>Example</th>
</tr>
</thead>
</table>
| []       | Range of letters or digits. To separate the start and end of a range, use a hyphen (- -). | [edit system login class test]  
user@host# set permissions clear  
user@host# set permissions configure  
user@host# set permissions network  
user@host# set permissions trace  
user@host# set permissions view  
user@host# set allow-configuration-regexp [“interfaces [gx]e-.* unit [0-9]*” description “”]  
With the above configuration, the users assigned to the test login class have operator-level user permissions, and have access to configure interfaces within the specified range of interface name and unit number (0 through 9). |
| ()       | A group of commands, indicating a complete, standalone expression to be evaluated. The result is then evaluated as part of the overall expression. Parentheses must be used in conjunction with pipe operators, as explained. | [edit system login class test]  
user@host# set permissions all  
user@host# set allow-commands “(clear)|(configure)”  
user@host# deny-commands “(mtrace)|(start)|(delete)”  
With the above configuration, users assigned to the test login class have superuser-level permissions, and have access to the commands specified in the allow-commands statement. |
| *        | Zero or more terms.                                                  | [edit system login class test]  
user@host# set permissions configure  
user@host# set deny-configuration “(system login class m*)”  
With the above configuration, users assigned to the test login class whose login username begins with m are denied configuration access. |
Table 8: Common Regular Expression Operators (continued)

<table>
<thead>
<tr>
<th>Operator</th>
<th>Match</th>
<th>Example</th>
</tr>
</thead>
</table>
| +        | One or more terms. | [edit system login class test]  
user@host# set permissions configure  
user@host# set deny-configuration "(system login class m+)"  
With the above configuration, users assigned to the test login class whose login username begins with m are denied configuration access. |
| .        | Any character except for a space " ". | [edit system login class test]  
user@host# set permissions configure  
user@host# set deny-configuration "(system login class m.)"  
With the above configuration, users assigned to the test login class whose login username begins with m are denied configuration access. |
| .*       | Everything from the specified point onward. | [edit system login class test]  
user@host# set permissions configure  
user@host# set deny-configuration "(system login class m .*)"  
With the above configuration, users assigned to the test login class whose login username begins with m are denied configuration access.  
Similarly, the deny-configuration "protocols .*" statement denies all configuration access under the [edit protocols] hierarchy level.  
NOTE:  
- The *, +, and . operations can be achieved by using .*.
- The deny-commands .* and deny-configuration .* statements deny access to all operational mode commands and configuration hierarchies, respectively. |

NOTE: Junos OS does not support the ! regular expression operator.

Regular Expression Examples

Table 9 on page 137 lists the regular expressions used to allow configuration options under two configuration hierarchies—[edit system ntp server] and [edit protocols rip]—as an example for specifying regular expressions.
NOTE: Table 9 on page 137 does not provide a comprehensive list of all regular expressions and keywords for all configuration statements and hierarchies. The regular expressions listed in the table are supported in Junos OS Release 16.1, and are validated only for the [edit system ntp server] and [edit protocols rip] statement hierarchies.

<table>
<thead>
<tr>
<th>Statement Hierarchy</th>
<th>Regular Expressions</th>
<th>Allowed Configuration</th>
<th>Denied Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[edit system ntp server]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>key key-number</td>
<td>[edit system login class test] set permissions configure set allow-configuration-regexps [ &quot;system ntp server .&quot; &quot;system ntp server . key .&quot; ] set deny-configuration-regexps [ &quot;system ntp server .&quot; version .&quot; &quot;system ntp server . prefer&quot; ]</td>
<td>• server IP</td>
<td>• version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• server IP and key</td>
<td>• prefer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• server IP and version</td>
<td>• prefer</td>
</tr>
<tr>
<td>prefer</td>
<td>[edit system login class test] set permissions configure set allow-configuration-regexps [ &quot;system ntp server .&quot; &quot;system ntp server . prefer&quot; ]; set deny-configuration-regexps [ &quot;system ntp server .&quot; key .&quot; &quot;system ntp server . version .&quot; ]</td>
<td>• server IP</td>
<td>• key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• server IP and prefer</td>
<td>• version</td>
</tr>
<tr>
<td>[edit protocols rip]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statement Hierarchy</td>
<td>Regular Expressions</td>
<td>Allowed Configuration</td>
<td>Denied Configuration</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| message-size        | [edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip message-size .*" set deny-configuration-regexps [ "protocols rip metric-in .*" "protocols rip route-timeout .*" "protocols rip update-interval .*" ] | • message-size | • metric-in  
|                     |                     |                       | • route-timeout  
|                     |                     |                       | • update-interval |
| metric-in           | [edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip metric-in .*" set deny-configuration-regexps [ "protocols rip message-size .*" "protocols rip route-timeout .*" "protocols rip update-interval .*" ] | • metric-in | • message-size  
|                     |                     |                       | • route-timeout  
|                     |                     |                       | • update-interval |
| route-timeout       | [edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip route-timeout .*" set deny-configuration-regexps [ "protocols rip metric-in .*" "protocols rip message-size .*" "protocols rip update-interval .*" ] | • route-timeout | • message-size  
|                     |                     |                       | • metric-in  
|                     |                     |                       | • update-interval |
| update-interval     | [edit system login class test] set permissions configure set allow-configuration-regexps "protocols rip update-interval .*" set deny-configuration-regexps [ "protocols rip metric-in .*" "protocols rip route-timeout .*" "protocols rip message-size .*" ] | • update-interval | • message-size  
|                     |                     |                       | • metric-in  
|                     |                     |                       | • route-timeout |
Examples of Defining Access Privileges Using allow-configuration and deny-configuration Statements

You can define access privileges using a combination of the following types of statements:

- permission flags
- allow-configuration and deny-configuration statements

The permission flags define the larger boundaries of what a person or login class can access and control. The allow-configuration and deny-configuration statements take precedence over permission flags and give the administrator finer control over exactly what the user has access to.

This topic explains defining access privileges using allow-configuration and deny-configuration statements by showing a series of examples of login class configuration using these statements. Examples 1 through 3 use both permission flags and deny-configuration statements to create login classes that allow users access to all except something. Each allow-configuration or deny-configuration statement is configured with one or more regular expressions to be allowed or denied.

Notice that permission bit and permission flag are used interchangeably.

Example 1

To create a login class that allows the user to configure everything except telnet parameters:

1. Set the user's login class permission bit to all.

   [edit system login]
   user@host# set class all-except-telnet permissions all

2. Include the following deny-configuration statement.

   [edit system login class all-except-telnet]
   user@host# set deny-configuration "system services telnet"

Example 2
To create a login class that allows the user to configure everything except anything within any login class whose name begins with "m":

1. Set the user's login class permission bit to all.

   
   [edit system login]
   user@host# set class all-except-login-class-m permissions all

2. Include the following deny-configuration statement.

   
   [edit system login class all-except-login-class-m]
   user@host# set deny-configuration "system login class m.*"

Example 3

This next example shows the creation of a login class with the all permission bit that prevents the user from editing a configuration or issuing commands (such as commit) at the [edit system login class] or [edit system services] hierarchy levels:

To create a login class that allows the user to configure everything except at the [edit system login class] or [edit system services] hierarchy levels:

1. Set the user's login class permission bit to all.

   
   [edit system login]
   user@host# set class all-except-login-class-or-system-services permissions all

2. Include the following deny-configuration statement.

   
   [edit system login class all-except-login-class-or-system-services]
   user@host# set deny-configuration "(system login class) | (system services)"

The next two examples show how to use the allow-configuration and deny-configuration statements to determine permissions inverse to each other for the [edit system services] hierarchy level.
**Example 4**

To create a login class that allows the user to have full configuration privileges at the [edit system services] hierarchy level and at only the [edit system services] hierarchy level:

1. Set the user’s login class permission bit to **configure**.

```
[edit system login]
user@host# set class configure-only-system-services permissions configure
```

2. Include the following **allow-configuration** statement.

```
[edit system login class configure-only-system-services]
user@host# set allow-configuration "system services"
```

**Example 5**

To create a login class that allows the user full permissions for all configuration mode hierarchies except the [edit system services] hierarchy level:

1. Set the user’s login class permission bit to **all**.

```
[edit system login]
user@host# set class all-except-system-services permissions all
```

2. Include the following **deny-configuration** statement.

```
[edit system login class all-except-system-services]
user@host# set deny-configuration "system services"
```
Example: Using Additive Logic With Regular Expressions to Specify Access Privileges

This example shows how to use additive logic when using regular expressions to set up configuration access privileges.

Requirements

This example uses the following hardware and software components:

- One Juniper Networks J Series, M Series, MX Series, or T Series device
- Junos OS Release 16.1 or later
  - There must be at least one user assigned to a login class.
  - There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview

To control who can make configuration changes to the system, and what specifically they can change, you can create regular expressions that indicate specific portions of the configuration hierarchy that users in a named user class are permitted to access. For example, you can create regular expressions that specify a group of routing instances that users are allowed to modify, and prevent the users from making changes to any other routing instances, or to any other configuration level.

You configure regular expressions using the `allow-configuration-regexp` and `deny-configuration-regexp` statements. By default, `deny-configuration-regexp` statements take precedence over `allow-configuration-regexp` statements for users in the named user class to which they are applied.

If a configuration hierarchy appears in a `deny-configuration-regexp` statement for a named user class, it is not visible to the users, regardless of the contents of the `allow-configuration-regexp` statement. If a
configuration hierarchy does not appear in a `deny-configuration-regexps` statement, it is visible if it appears in an `allow-configuration-regexps` statement, or if there is no `allow-configuration-regexps` statement configured for the user class.

You can optionally change this default behavior so additive logic (that is, deny all by default / allow some as specified) is used in regular expressions. When additive logic is enabled, the behavior of existing regular expressions changes so that all configuration hierarchies are denied unless they are included in an `allow-configuration-regexps` statement for the named user class.

**Configuration**

To enable additive logic for regular expressions:

1. To explicitly allow one or more individual configuration mode hierarchies, include the `allow-configuration-regexps` statement at the `[edit system login class class-name]` hierarchy level, configured with the regular expressions to be allowed.

   ```
   [edit system login class class-name]
   user@host# set allow-configuration-regexps "regular expression 1" "regular expression 2" "regular expression 3" "regular expression 4" ...
   ```

2. Assign the login class to one or more users.

   ```
   [edit system login]
   user@host# set user username class class-name
   ```

3. Enable additive logic for regular expressions.

   ```
   [edit system]
   user@host# set regex-additive-logic
   ```

4. Commit your changes.

   Users assigned this login class have access to the configuration hierarchies included in the `allow-configuration-regexps` statement, but no others.

**Examples**

*Using Regular Expressions with Additive Logic*

**Purpose**
This section provides examples of regular expressions that use additive logic to give you ideas for creating configurations appropriate for your system.

**Allow Specific Routing Instances**

The following example login class includes a regular expression that allows configuration of routing instances whose names start with `CUST-VRF-`; for example, `CUST-VRF-1`, `CUST-VRF-25`, `CUST-VRF-100`, and so on:

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "routing-instances CUST-VRF-.*.*"
```

If the following statement is included in the configuration, it prevents the user from configuring any other routing instances and denies access to any non-routing instance configuration hierarchy:

```
[edit system]
user@host# set regex-additive-logic
```

**Allow BGP Peer Configuration Only**

The following example login class includes a regular expression that allows configuration of BGP peers:

```
[edit system login class class-name]
user@host# set permissions configure view view-configuration
user@host# set allow-configuration-regexps "protocols bgp group *"
```

If the following statement is included in the configuration, it prevents the user from making any other changes, such as deleting or disabling BGP statements:

```
[edit system]
user@host# set regex-additive-logic
```

**Verification**
To verify that you have set the access privileges correctly:

1. Configure a login class and commit the changes.

2. Assign the login class to a username.

3. Log in as the username assigned with the new login class.

4. Attempt to perform the configurations that have been allowed.
   - You should be able to perform configuration changes to hierarchy levels and regular expressions that have been allowed.
   - All other hierarchies should not be visible.
   - Any allowed or denied expressions should take precedence over any permissions granted with the permissions statement.

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands

This example shows how to configure custom login classes and assign access privileges for operational mode commands. This enables users of the customized login class to execute only those operational commands for which access privileges have been specified. This prevents unauthorized users from executing sensitive commands that could potentially cause damage to the network.
Requirements

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

  For information on configuring a TACACS+ server, see “Configuring TACACS+ Authentication” on page 264.

- Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview and Topology

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the permissions statement at the [edit system login class class-name] hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the permissions statement. In addition to this, you can specify extended regular expressions with the following statements:

- allow-commands and deny-commands—Allow or deny access to operational mode commands only.
- allow-configuration and deny-configuration—Allow or deny access to a particular configuration hierarchy only.
- allow-configuration-regexp and deny-configuration-regexp—Allow or deny access to a particular configuration hierarchy using strings of regular expressions.
- allow-commands-regexp and deny-commands-regexp—(TACACS+ authorization only) Allow or deny access to a particular command using strings of regular expressions.

The above statements define a user’s access privileges to individual operational mode commands, configuration statements, and hierarchies. These statements take precedence over the login class permissions set for a user.
Configuration Notes

When configuring the allow-commands, deny-commands, allow-configuration, and deny-configuration statements with access privileges, take the following into consideration:

- You can include the allow/deny statement only once in each login class.
- If the exact same command is configured under both allow-commands and deny-commands statements, or both allow-configuration and deny-configuration statements, then the allow operation takes precedence over the deny statement.

For instance, with the following configuration, a user assigned to login class test is allowed to install software using the request system software add command, although the deny-commands statement also includes it:

```
[edit system login]
user@host# set class test permissions allow-commands "request system software add"
user@host# set class test permissions deny-commands "request system software add"
```

For instance, with the following configuration, a user assigned to login class test is allowed to access the [edit system services] configuration hierarchy, although the deny-configuration statement also includes it:

```
[edit system login]
user@host# set class test permissions allow-configuration "system services"
user@host# set class test permissions deny-configuration "system services"
```

- If you specify a regular expression for allow-commands and deny-commands statements with two different variants of a command, the longest match is always executed.

For instance, for the following configuration, a user assigned to test login class is allowed to execute the commit synchronize command and not the commit command. This is because commit-synchronize is the longest match between commit and commit-synchronize, and it is specified for allow-commands.

```
[edit system login]
user@host# set class test allow-commands "commit-synchronize"
user@host# set class test deny-commands commit
```

- Regular expressions for allow-commands and deny-commands statements can also include the commit, load, rollback, save, status, and update commands.
- Explicitly allowing configuration mode hierarchies or regular expressions using the allow-configuration statement adds to the regular permissions set using the permissions statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the deny-configuration statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the permissions statement.
For example, for the following configuration, the login class user can edit the configuration at the [edit system services] hierarchy level and issue configuration mode commands (such as commit), in addition to just entering the configuration mode using the configure command, which is the permission specified by the configure permission flag:

```
[edit system login]
user@host# set class test permissions configure allow-configuration "system services"
```

Likewise, for the following configuration, the login class user can perform all operations allowed by the all permissions flag, except issuing configuration mode commands (such as commit) or modifying the configuration at the [edit system services] hierarchy level:

```
[edit system login]
user@host# set class test permissions all deny-configuration "system services"
```

- The allow/deny-configuration statements are mutually exclusive with the allow/deny-configuration-regexps statements, and the allow/deny-commands statements are mutually exclusive with the allow/deny-commands-regexps statements. For example, you cannot configure both allow-configuration and allow-configuration-regexps in the same login class.

- If you have existing configurations using the allow/deny-configuration or allow/deny-commands statements, using the same configuration options with the allow/deny-configuration-regexps or allow/deny-commands-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

- To define access privileges to parts of the configuration hierarchy, specify the full paths in the extended regular expressions with the allow-configuration and deny-configuration statements. Use parentheses around an extended regular expression that connects two or more expressions with the pipe (|) symbol.

For example:

```
[edit system login]
user@host# set class test deny-configuration "(system login class) | (system services)"
```

- If the regular expression contains any spaces, operators, or wildcard characters, enclose the expression in quotation marks. Regular expressions are not case-sensitive; for example, allow-commands "show interfaces".

- Modifiers such as set, log, and count are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

Incorrect configuration:

```
[edit system login]
user@host# set class test permission deny-commands "set protocols"
```
Correct configuration:

```
[edit system login]
user@host# set class test permission deny-commands protocols
```

- Anchors are required when specifying complex regular expressions with the `allow-commands` statement. For example:

```
[edit system login]
user@host# set class test permissions allow-commands "(^monitor) | (^ping) | (^show) | (^exit)"

OR

set class test permissions allow-commands "allow-commands ="^(monitor | ping | show | exit)"
```

- When specifying extended regular expressions using the `allow/deny-commands` and `allow/deny-configuration` statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol. For example:

```
[edit system login]
user@host# set class test allow-commands "(ping .*)|(traceroute .*)|(show .*)|(configure .*)|(edit)|(exit)|(commit)|(rollback .*)"

user@host# set class test deny-configuration "(system login class)|(system services)"
```

- When specifying extended regular expressions using the `allow/deny-configuration-regexps` or `allow/deny-commands-regexps` statement, each expression enclosed within quotes (") and separated by a space must be enclosed in angular brackets [ ]. For example:

```
[edit system login]
user@host# set class test allow-configuration-regexps [ "interfaces . * description . *" "interfaces . * unit . * description . *" "interfaces . * unit . * family inet address . *"]
```

- You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use [ * ] or [ .* ] alone.

- You cannot configure the `allow-configuration` statement with the `(interfaces (description (.*)) regular expression, as this evaluates to `allow-configuration = .*` regular expression.

- You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.
Figure 1 on page 150 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

In this example, R1 is configured with three customized login classes—Class1, Class2, and Class3—for specifying access privileges with extended regular expressions using the allow-commands and deny-commands statements differently.

The purpose of each login class is as follows:

- **Class1**—Defines access privileges for the user with the allow-commands statement only. This login class provides operator-level user permissions, and should provide authorization for only rebooting the device.

- **Class2**—Defines access privileges for the user with the deny-commands statement only. This login class provides operator-level user permissions, and should deny access to set commands.

- **Class3**—Defines access privileges for the user with both the allow-commands and deny-commands statements. This login class provides superuser-level user permissions, and should provide authorization for accessing interfaces and viewing device information. It should also deny access to edit and configure commands.

Router R1 has three different users, User1, User2, and User3, assigned to Class1, Class2, and Class3 login classes, respectively.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
R1

set system authentication-order tacplus
set system authentication-order radius
```
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66
set system login class Class1 permissions clear
set system login class Class1 permissions network
set system login class Class1 permissions reset
set system login class Class1 permissions trace
set system login class Class1 permissions view
set system login class Class1 allow-commands "request system reboot"
set system login class Class2 permissions clear
set system login class Class2 permissions network
set system login class Class2 permissions reset
set system login class Class2 permissions trace
set system login class Class2 permissions view
set system login class Class2 deny-commands set
set system login class Class3 permissions all
set system login class Class3 allow-commands configure
set system login class Class3 deny-commands .*
set system login user User1 uid 2001
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2002
set system login user User2 class Class2
set system login user User2 authentication encrypted-password "$ABC123"
set system login user User3 uid 2003
set system login user User3 class Class3
set system login user User3 authentication encrypted-password "$ABC123"
set system syslog file messages any any

Configuring Authentication Parameters for Router R1

Step-by-Step Procedure
The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure Router R1 authentication:

1. Configure the order in which authentication should take place for R1. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, and then the local password.

```
[edit system]
user@R1# set authentication-order tacplus
user@R1# set authentication-order radius
user@R1# set authentication-order password
```

2. Establish R1 connection with the TACACS+ server.

```
[edit system]
user@R1# set tacplus-server 10.209.1.66
user@R1# set tacplus-options enhanced-accounting
user@R1# set accounting destination tacplus server 10.209.1.66
```

3. Configure RADIUS server authentication parameters.

```
[edit system]
user@R1# set radius-server 10.209.1.66 secret "$ABC123"
user@R1# set radius-options enhanced-accounting
```

4. Configure R1 accounting configuration parameters.

```
[edit system]
user@R1# set accounting events login
user@R1# set accounting events change-log
user@R1# set accounting events interactive-commands
user@R1# set accounting traceoptions file auditlog
user@R1# set accounting traceoptions flag all
```

**Configuring Access Privileges with allow-commands Statement Only (Class1)**

**Step-by-Step Procedure**

To specify regular expressions using the `allow-commands` statement only:

1. Configure Class1 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 69.
2. Specify the command to enable rebooting of R1 in the `allow-commands` statement.

```
[edit system login]
user@R1# set class Class1 allow-commands "request system reboot"
```

3. Configure the user account for the Class1 login class.

```
[edit system login]
user@R1# set user User1 uid 2001
user@R1# set user User1 class Class1
user@R1# set user User1 authentication encrypted-password "$ABC123"
```

### Configuring Access Privileges with `deny-commands` Statement Only (Class2)

**Step-by-Step Procedure**

To specify regular expressions using the `deny-commands` statement only:

1. Configure the Class2 custom login class and assign operator-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 69.

```
[edit system login]
user@R1# set class Class1 permissions clear
user@R1# set class Class1 permissions network
user@R1# set class Class1 permissions reset
user@R1# set class Class1 permissions trace
user@R1# set class Class1 permissions view
```

2. Disable execution of any set commands in the `deny-commands` statement.

```
[edit system login]
user@R1# set class Class1 deny-commands "set"
```

3. Configure the user account for the Class2 login class.
Configuring Access Privileges with Both allow-commands and deny-commands Statements (Class3)

Step-by-Step Procedure
To specify regular expressions using both the allow-commands and deny-commands statements:

1. Configure the Class3 custom login class and assign superuser-level user permissions. For information on the predefined system login classes, see the "Junos OS Login Classes Overview" on page 69.

   [edit system login]
   user@R1# set class Class3 permissions all

2. Specify the commands to enable only configure commands in the allow-commands statement.

   [edit system login]
   user@R1# set class Class3 allow-commands configure

3. Disable execution of all commands in the deny-commands statement.

   [edit system login]
   user@R1# set class Class3 deny-commands .*

4. Configure the user account for the Class1 login class.

   [edit system login]
   user@R1# set login user User3 uid 2003
   user@R1# set login user User3 class Class3
   user@R1# set login user User3 authentication encrypted-password "$ABC123"

Results
From configuration mode, confirm your configuration by entering the show system command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

   user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
    10.209.1.66 secret "$ABC123";
}
tacplus-server {
    10.209.1.66;
}
radius-options {
    enhanced-accounting;
}
tacplus-options {
    enhanced-accounting;
}
accounting {
    events [ login change-log interactive-commands ];
    traceoptions {
        file auditlog;
        flag all;
    }
    destination {
        tacplus {
            server {
                10.209.1.66;
            }
        }
    }
}
login {
    class Class1 {
        permissions [ clear network reset trace view ];
        allow-commands "request system reboot";
    }
    class Class2 {
        permissions [ clear network reset trace view ];
        deny-commands set;
    }
    class Class3 {
        permissions all;
        allow-commands configure;
        deny-commands ";."
    }
    user User1 {
        uid 2001;
        class Class1;
Login as the username assigned with the new login class, and confirm that the configuration is working properly.

*Verifying Class 1 Configuration*

**Purpose**

Verify that the permissions and commands allowed in the Class1 login class are working.
Action

From operational mode, run the **show system users** command.

User1@R1>  **show system users**

```
12:39PM  up 6 days, 23 mins, 6 users, load averages: 0.00, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE  WHAT
User1  p0       abc.example.net 12:34AM 12:04 cli
User2  p1       abc.example.net 12:36AM 12:02 -cli (cli)
User3  p2       abc.example.net 10:41AM    11 -cli (cli)
```

From operational mode, run the **request system reboot** command.

User1@R1>  **request system ?**

```
Possible completions:
reboot               Reboot the system
```

Meaning

The Class1 login class to which User1 is assigned has the operator-level user permissions, and is allowed to execute the **request system reboot** command.

The predefined operator login class has the following permission flags specified:

- **clear**—Can clear (delete) information learned from the network that is stored in various network databases by using the **clear** commands.
- **network**—Can access the network by using the **ping**, **ssh**, **telnet**, and **traceroute** commands.
- **reset**—Can restart software processes by using the **restart** command and can configure whether software processes are enabled or disabled at the **[edit system processes]** hierarchy level.
- **trace**—Can view trace file settings and configure trace file properties.
- **view**—Can use various commands to display current system-wide, routing table, and protocol-specific values and statistics. Cannot view the secret configuration.

For the Class1 login class, in addition to the above-mentioned user permissions, User1 can execute the **request system reboot** command. The first output displays the view permissions as an operator, and the second output shows that the only **request** command that User1 can execute as an operator is the **request system reboot** command.

**Verifying Class2 Configuration**

Purpose
Verify that the permissions and commands allowed for the Class2 login class are working.

**Action**

From the operational mode, run the `ping` command.

```
User2@R1> ping 10.209.1.66
```

```
ping 10.209.1.66
PING 10.209.1.66 (10.209.1.66): 56 data bytes
64 bytes from 10.209.1.66: icmp_seq=0 ttl=52 time=212.521 ms
64 bytes from 10.209.1.66: icmp_seq=1 ttl=52 time=212.844 ms
64 bytes from 10.209.1.66: icmp_seq=2 ttl=52 time=211.304 ms
64 bytes from 10.209.1.66: icmp_seq=3 ttl=52 time=210.963 ms
^C
--- 10.209.1.66 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 210.963/211.908/212.844/0.792 ms
```

From the CLI prompt, check the available permissions.

```
User2@R1> ?
```

```
Possible completions:
clear Clear information in the system
file Perform file operations
help Provide help information
load Load information from file
monitor Show real-time debugging information
mtrace Trace multicast path from source to receiver
op Invoke an operation script
ping Ping remote target
quit Exit the management session
request Make system-level requests
restart Restart software process
save Save information to file
show Show system information
ssh Start secure shell on another host
start Start shell
telnet Telnet to another host
```
test Perform diagnostic debugging
traceoute Trace route to remote host

From the CLI prompt, execute any set command.

User2@R1> set

^ unknown command.

**Meaning**
The Class2 login class to which User2 is assigned has the operator-level user permissions, and is denied access to all `set` commands. This is displayed in the command outputs.

The permission flags specified for the predefined operator login class are the same as that of Class1.

**Verifying Class3 Configuration**

**Purpose**
Verify that the permissions and commands allowed for the Class3 login class are working.

**Action**
From the CLI prompt, check the available permissions.

User3@R1> ?

Possible completions:
  configure Manipulate software configuration information

From the operational mode, enter configuration mode.

User3@R1> configure

Entering configuration mode

[edit]
User3@R1#

**Meaning**
The Class3 login class to which User3 is assigned has the superuser (all) user permissions, but is allowed to execute the `configure` command only, and is denied access to all other operational mode commands. Because the regular expressions specified in the `allow/deny-commands` statements take precedence over the user permissions, User3 on R1 has access only to configuration mode, and is denied access to all other operational mode commands.

**Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies**

This example shows how to configure custom login classes and assign access privileges to portions of the configuration hierarchy. This enables users of the customized login class to execute only those configuration statements and hierarchies for which access privileges have been specified. This prevents unauthorized users from accessing device configurations that could potentially cause damage to the network.

**Requirements**

This example uses the following hardware and software components:

- One Juniper Networks device
- One TACACS+ (or RADIUS) server
- Junos OS build running on the Juniper Networks device

Before you begin:

- Establish a TCP connection between the device and the TACACS+ server. In the case of the RADIUS server, establish a UDP connection between the device and the RADIUS server.

  For information on configuring a TACACS+ server, see "Configuring TACACS+ Authentication" on page 264.
• Configure at least one user assigned to a login class on the Juniper Networks device. There can be more than one login class, each with varying permission configurations, and more than one user on the device.

Overview and Topology

Each top-level command-line interface (CLI) command and each configuration statement in Junos OS has an access privilege level associated with it. For each login class, you can explicitly deny or allow the use of operational and configuration mode commands that would otherwise be permitted or not allowed by a privilege level. Users can execute only those commands and configure and view only those statements for which they have access privileges. To configure access privilege levels, include the permissions statement at the [edit system login class class-name] hierarchy level.

The access privileges for each login class are defined by one or more permission flags specified in the permissions statement. In addition to this, you can specify extended regular expressions with the following statements:

• allow-commands and deny-commands—Allow or deny access to operational mode commands.

• allow-configuration and deny-configuration—Allow or deny access to parts of the configuration hierarchy.

These statements perform slower matching, with more flexibility, especially in wildcard matching. However, it can take a very long time to evaluate all of the possible statements if a great number of full-path regular expressions or wildcard expressions are configured, possibly impacting performance.

• allow-configuration-regexps and deny-configuration-regexps—Allow or deny access to a particular configuration hierarchy using strings of regular expressions. These statements are similar to allow-configuration and deny-configuration statements, except that in the allow/deny-configuration-regexps statements you can configure sets of strings in which the strings include spaces when using the first set of statements.

The above statements define a user’s access privileges to individual operational mode commands, configuration statements, and hierarchies. These statements take precedence over a login class permissions bit set for a user.

Difference between allow/deny-configuration and allow/deny-configuration-regexps statements

The allow-configuration and deny-configuration statements were introduced before Junos OS Release 7.4. The allow-configuration-regexps and deny-configuration-regexps statements were introduced in Junos OS Release 11.2. In Junos OS Release 11.4, the allow-configuration and deny-configuration statements were deprecated, but because these statements were useful in executing simple configurations, these statements were undeprecated in Junos OS Release 11.4R6, and starting with the 11.4R6 release, both the allow/deny-configuration and the allow/deny-configuration-regexps statements are supported.

The allow/deny-configuration-regexps statements split up the regular expression into tokens and match each piece against each part of the specified configuration’s full path, whereas the allow/deny-configuration statements match against the full string. For allow/deny-configuration-regexps statements, you configure
a set of strings in which each string is a regular expression, with spaces between the terms of the string. This provides very fast matching, but with less flexibility. For specifying wildcard expressions you must set up wildcards for each token of the space-delimited string you want to match, and this makes it more tedious to use wildcard expressions for these statements.

For example:

- This example shows that **options** is the only matched expression against the first token of the statement.

  ```
  [edit system]
  login {
    class test {
      permissions configure;
      allow-configuration-regexp .*options;
    }
  }
  ```

  The above configuration matches the following statements:
  
  - set policy-**options** condition **condition** dynamic-db
  - set routing-**options** static route **static-route** next-hop **next-hop**
  - set event-**options** generate-event **event** time-interval **seconds**

  The above configuration does not match the following statements:

  - system host-name host-**options**
  - interfaces *interface-name* description **options**

- This example shows that **ssh** is the only matched expression against the third token of the statement.

  ```
  [edit system]
  login {
    class test {
      permissions configure;
      allow-configuration-regexp ".*.*.*ssh";
    }
  }
  ```

  In the above example, the three tokens include .*.*, and .*ssh, respectively.

  The above configuration matches the following statements:

  - system host-name hostname-**ssh**
  - system services **ssh**
  - system services outbound-**ssh**
The above configuration does not match the following statement:

- interfaces interface-name description ssh

You can restrict configuration access easily using the `deny-configuration` statement as compared to using the `deny-configuration-regexps` statement. Table 10 on page 163 illustrates the use of both the `deny-configuration` and `deny-configuration-regexps` statements in different configurations to achieve the same result of restricting access to a particular configuration.

Table 10: Restricting Configuration Access Using `deny-configuration` and `deny-configuration-regexps` Statements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>xnm-ssl</td>
<td>[edit system]</td>
<td>[edit system]</td>
<td>The following configuration statement is denied:</td>
</tr>
<tr>
<td></td>
<td>login {</td>
<td>login {</td>
<td>• system services xnm-ssl</td>
</tr>
<tr>
<td></td>
<td>class test {</td>
<td>class test {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>permissions configure;</td>
<td>permissions configure;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>allow-configuration.*;</td>
<td>allow-configuration.*;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>deny-configuration.*xnm-ssl;</td>
<td>deny-configuration-regexps &quot;.*.*xnm-ssl&quot;;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ssh</td>
<td>[edit system]</td>
<td>[edit system]</td>
<td>The following configuration statements are denied:</td>
</tr>
<tr>
<td></td>
<td>login {</td>
<td>login {</td>
<td>• system services ssh</td>
</tr>
<tr>
<td></td>
<td>class test {</td>
<td>class test {</td>
<td>• system services outbound-ssh</td>
</tr>
<tr>
<td></td>
<td>permissions configure;</td>
<td>permissions configure;</td>
<td>• system services ssh</td>
</tr>
<tr>
<td></td>
<td>allow-configuration.*;</td>
<td>allow-configuration.*;</td>
<td>• security ssh-known-host</td>
</tr>
<tr>
<td></td>
<td>deny-configuration.*ssh;</td>
<td>deny-configuration-regexps &quot;.*ssh&quot;;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

Although the `allow/deny-configuration` statements are also useful when simple configuration is desired, the `allow/deny-configuration-regexps` statements provide better performance and overcome the ambiguity that existed when combining expressions set in the `allow/deny-configuration` statements.
NOTE: The allow/deny-configuration and allow/deny-configuration-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-configuration statement, or the allow/deny-configuration-regexps statement. If you have existing configurations using the allow/deny-configuration statements, using the same configuration options with the allow/deny-configuration-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Configuration Notes

When configuring the allow-configuration, deny-configuration, allow-configuration-regexps, and deny-configuration-regexps statements with access privileges, take the following into consideration:

- You can include one deny-configuration and one allow-configuration statement in each login class.
- The allow/deny-configuration and allow/deny-configuration-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-configuration statement, or the allow/deny-configuration-regexps statement. If you have existing configurations using the allow/deny-configuration statements, using the same configuration options with the allow/deny-configuration-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

- Explicitly allowing configuration mode hierarchies or regular expressions using the allow-configuration statement adds to the regular permissions set using the permissions statement. Likewise, explicitly denying configuration mode hierarchies or regular expressions using the deny-configuration statement removes permissions for the specified configuration mode hierarchy, from the default permissions provided by the permissions statement.

For example, for the following configuration, the login class user can edit the configuration at the [edit system services] hierarchy level and issue configuration mode commands (such as commit), in addition to just entering the configuration mode using the configure command, which is the permission specified by the configure permission flag:

```
[edit system login]
user@host# set class test permissions configure allow-configuration "system services"
```

Likewise, for the following configuration, the login class user can perform all operations allowed by the all permissions flag, except issuing configuration mode commands (such as commit) or modifying the configuration at the [edit system services] hierarchy level:

```
[edit system login]
user@host# set class test permissions all deny-configuration "system services"
```
• To define access privileges to parts of the configuration hierarchy, specify the full paths in the extended regular expressions with the `allow-configuration` and `deny-configuration` statements. Use parentheses around an extended regular expression that connects two or more expressions with the pipe (`|`) symbol.

For example:

```
[edit system login]
user@host# set class test deny-configuration "(system login class)(system services)"
```

• When specifying extended regular expressions using the `allow/deny-commands` and `allow/deny-configuration` statements, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

For example:

```
[edit system login]
user@host# set class test allow-commands "(ping .*)|(traceroute .*)|(show .*)|(configure .*)|(edit)|(exit)|(commit)|(rollback .*)"
user@host# set class test deny-configuration "(system login class)(system services)"
```

• When specifying extended regular expressions using the `allow-deny-configuration-regexps` statement, each expression enclosed within quotes (`) and separated by a space must be enclosed in angular brackets [ ].

For example:

```
[edit system login]
user@host# set class test allow-configuration-regexps [ "interfaces.* description.*" "interfaces.* unit.* description.*" "interfaces.* unit.* family inet address.*" ]
```

• If the exact same command is configured under both `allow-configuration` and `deny-configuration` statements, then the allow operation takes precedence over the deny statement.

For instance, with the following configuration, a user assigned to login class test is allowed to access the [edit system services] configuration hierarchy, although the `deny-configuration` statement also includes it:

```
[edit system login]
user@host# set class test permissions allow-configuration "system services"
user@host# set class test permissions deny-configuration "system services"
```

For instance, if a certain command or configuration is allowed, for example, using permission `all`, then we can use the `deny-configuration` command to deny access to a particular hierarchy.
• Modifiers such as set, log, and count are not supported within the regular expression string to be matched. If a modifier is used, then nothing is matched.

Incorrect configuration:

```bash
[edit system login]
user@host# set class test permission deny-configuration "set protocols"
```

Correct configuration:

```bash
[edit system login]
user@host# set class test permission deny-configuration protocols
```

• You can use the * wildcard character when denoting regular expressions. However, it must be used as a portion of a regular expression. You cannot use [ * ] or [ .* ] alone.

• You cannot configure the allow-configuration statement with the (interfaces (description [.*]) regular expression, as this evaluates to allow-configuration = .* regular expression.

• You can configure as many regular expressions as needed to be allowed or denied. Regular expressions to be denied take precedence over configurations to be allowed.

**Topology**

Figure 2: Configuring TACACS+ Server Authentication

Figure 2 on page 166 illustrates a simple topology, where Router R1 is a Juniper Networks device and has a TCP connection established with a TACACS+ server.

In this example, R1 is configured with two customized login classes—Class1 and Class2—for specifying access privileges with extended regular expressions using the allow-configuration, deny-configuration, allow-configuration-regexps, and deny-configuration-regexps statements differently.

The purpose of the login classes is as follows:

• **Class1**—Define access privileges for the user with the allow-configuration and deny-configuration statements. This login class should provide access to configure interfaces hierarchy only, and deny all other access on the device. To do this, the user permissions should include configure to provide configuration access. In addition to this, the allow-configuration statement should allow interfaces configuration, and the deny-configuration statement should deny access to all other configurations.
Because the allow statement takes precedence over the deny statement, the users assigned to the Class1 login class can access only the [edit interfaces] hierarchy level.

- **Class2**—Define access privileges for the user with the `allow-configuration-regexp` and `deny-configuration-regexp` statements. This login class provides superuser-level user permissions, and in addition, explicitly allows configuration under multiple hierarchy levels for interfaces. It also denies configuration access to the [edit system] and [edit protocols] hierarchy levels.

Router R1 has two users, User1 and User2, assigned to the Class1 and Class2 login classes, respectively.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

```
R1

set system authentication-order tacplus
set system authentication-order radius
set system authentication-order password
set system radius-server 10.209.1.66 secret "$ABC123"
set system tacplus-server 10.209.1.66
set system radius-options enhanced-accounting
set system tacplus-options enhanced-accounting
set system accounting events login
set system accounting events change-log
set system accounting events interactive-commands
set system accounting traceoptions file auditlog
set system accounting traceoptions flag all
set system accounting destination tacplus server 10.209.1.66
set system login class Class1 permissions configure
set system login class Class1 allow-configuration "interfaces .* unit .*"
set system login class Class1 deny-configuration .*
set system login class Class2 permissions all
set system login class Class2 allow-configuration-regexp [ "interfaces .* description .*" "interfaces .* unit .* description .*"]" "interfaces .* unit .* family inet address .*
set system login class Class2 deny-configuration-regexp [ "system" "protocols" ]
set system login user User1 uid 2004
set system login user User1 class Class1
set system login user User1 authentication encrypted-password "$ABC123"
set system login user User2 uid 2006
```
Configuring Authentication Parameters for Router R1

Step-by-Step Procedure
The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure Router R1 authentication:

1. Configure the order in which authentication should take place for R1. In this example, TACACS+ server authentication is first, followed by RADIUS server authentication, then the local password.

   ```
   [edit system]
   user@R1# set authentication-order tacplus
   user@R1# set authentication-order radius
   user@R1# set authentication-order password
   ```

2. Establish R1 connection with the TACACS+ server.

   ```
   [edit system]
   user@R1# set tacplus-server 10.209.1.66
   user@R1# set tacplus-options enhanced-accounting
   user@R1# set accounting destination tacplus server 10.209.1.66
   ```

3. Configure RADIUS server authentication parameters.

   ```
   [edit system]
   user@R1# set radius-server 10.209.1.66 secret "$ABC123"
   user@R1# set radius-options enhanced-accounting
   ```

4. Configure the R1 accounting configuration parameters.

   ```
   [edit system]
   user@R1# set accounting events login
   user@R1# set accounting events change-log
   user@R1# set accounting events interactive-commands
   ```
Configuring Access Privileges with allow-configuration and deny-configuration Statements (Class1)

Step-by-Step Procedure

To specify regular expressions using the allow-configuration and deny-configuration statements:

1. Configure the Class1 custom login class and assign configuration user permissions.

```plaintext
[edit system login]
user@R1# set class Class1 permissions configure
```

2. Specify the regular expression in the allow-configuration statement to allow configuration at the [edit interfaces] hierarchy level. To allow set commands at the [edit interfaces] hierarchy level, the regular expression used is `interfaces .* unit .*`.

```plaintext
[edit system login]
user@R1# set class Class1 allow-configuration "interfaces .* unit .*"
```

3. Specify the regular expression in the deny-configuration statement to disable all configuration access. The regular expression used to deny all configuration access is ".*".

```plaintext
[edit system login]
user@R1# set class Class1 deny-configuration ".*"
```

4. Configure the user account for the Class1 login class.

```plaintext
[edit system login]
user@R1# set system login user User1 uid 2004
user@R1# set system login user User1 class Class1
user@R1# set system login user User1 authentication encrypted-password "$ABC123"
```

Configuring Access Privileges with allow-configuration-regexp and deny-configuration-regexp Statements (Class2)

Step-by-Step Procedure
To specify regular expressions using the `allow-configuration-regexps` and `deny-configuration-regexps` statements:

1. Configure the Class2 custom login class and assign superuser (all) user permissions. For information on the predefined system login classes, see “Junos OS Login Classes Overview” on page 69.

```
[edit system login]
user@R1# set class Class2 permissions all
```

2. Specify the regular expression to allow access to multiple hierarchies under the `[edit interfaces]` hierarchy level.

```
[edit system login]
user@R1# set class Class2 allow-configuration-regexps [ "interfaces.* description.*" "interfaces.* unit.*
description.*" "interfaces.* unit.* family inet address.*" "interfaces.* disable"]
```

3. Specify the regular expression to deny configuration at the `[edit system]` and `[edit protocols]` hierarchy levels.

```
[edit system login]
user@R1# set class Class2 deny-configuration-regexps [ "system" "protocols" ]
```

4. Configure the user account for the Class2 login class.

```
[edit system login]
user@R1# set system login user User2 uid 2006
user@R1# set system login user User2 class Class2
user@R1# set system login user User2 authentication encrypted-password "$ABC123"
```

**Results**

From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show system
authentication-order [ tacplus radius password ];
radius-server {
  10.209.1.66 secret "$ABC123";
}
```
tacplus-server {
  10.209.1.66;
}
radius-options {
  enhanced-accounting;
}
tacplus-options {
  enhanced-accounting;
}
accounting {
  events [ login change-log interactive-commands ];
  traceoptions {
    file auditlog;
    flag all;
  }
  destination {
    tacplus {
      server {
        10.209.1.66;
      }
    }
  }
}
login {
  class Class1 {
    permissions configure;
    allow-configuration "interfaces.* unit.*";
    deny-configuration ".";
  }
  class Class2 {
    permissions all;
    allow-configuration-regexp [ "interfaces.* description.*" "interfaces.* unit.* description.*" "interfaces.* unit.* family inet address.*" "interfaces.* disable" ];
    deny-configuration-regexp [ "system" "protocols" ];
  }
  user User1 {
    uid 2001;
    class Class1;
    authentication {
      encrypted-password "$ABC123";
    }
  }
  user User2 {
    uid 2002;
  }
Log in as the username assigned with the new login class, and confirm that the configuration is working properly.

**Verifying Class1 Configuration**

**Purpose**

Verify that the permissions allowed in the Class1 login class are working.

**Action**

From the CLI prompt, check the available permissions.

```
User1@R1> ?
```

Possible completions:
```
clear                Clear information in the system
configure            Manipulate software configuration information
file                 Perform file operations
help                 Provide help information
load                 Load information from file
op                   Invoke an operation script
```
From the configuration mode, check the available configuration permissions.

User1@R1# edit?

Possible completions:
> interfaces  Interface configuration

Meaning
User1 has configure user permissions seen in the first output, and the only configuration access allowed for User1 is at the interfaces hierarchy level. All other configuration is denied, as seen in the second output.

Verifying Class2 Configuration

Purpose
Verify that the Class2 configuration is working.

Action
From the configuration mode, access the interfaces configuration.

[edit interfaces]
User2@R1# set?

Possible completions:
<interface-name>  Interface name
+ apply-groups    Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
ge-0/0/3  Interface name
> interface-range  Interface ranges configuration
> interface-set    Logical interface set configuration
> traceoptions     Interface trace options

From the configuration mode, access the system and protocols configuration hierarchies.

User2@R1# edit system
User2@R1# edit protocols

Meaning
User2 has permissions to configure interfaces of R1, but the [edit system] and [edit protocols] hierarchy levels are denied access, as seen in the output.

SEE ALSO
Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies | 128

RELATED DOCUMENTATION
Junos OS Login Classes Overview | 69
Junos OS User Accounts | 91
CHAPTER 3

Passwords for User Access

Root Password | 177
Recovering Root Password | 183
Plain-Text Passwords | 196
Master Password for Configuration Encryption | 200
Root Password

When the router, switch, or security device is powered on first time, it is ready to be configured. Initially, you log in as the user root with no password. Later, you must configure a plain-text password for the root-level user (whose username is root). Configuring a plain-text password is one way to protect access to the root level by unauthorized users. If you forget the root password for the router, you can use the password recovery procedure to reset the root password. Read this topic for more information.

Configuring the Root Password

The Junos OS is preinstalled on the router or switch. When the router or switch is powered on, it is ready to be configured. Initially, you log in as the user root with no password. The root directory of a UNIX device is the entry point to all other folders and files on that device. As a result, access to the root directory is restricted by default to a predefined user account known as the root user. The root user (also referred to as superuser) has unrestricted access and full permissions within the system. The expression "log in as root" is commonly used when an action requires the user to log into the device as the root user.

**NOTE:** If you configure a blank password using the encrypted-password statement at the [edit system root-authentication] hierarchy level for root authentication, you can commit a configuration but you cannot log in as the root user and gain root level access to the router or switch.

After you log in, you should configure the root (superuser) password by including the root-authentication statement at the [edit system] hierarchy level and configuring one of the password options:
If you configure the **plain-text-password** option, you are prompted to enter and confirm the password:

```
[edit system]
user@host# set root-authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

The default requirements for plain-text passwords are:

- The password must be between 6 and 128 characters long
  - You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
  - Valid passwords must contain at least one uppercase letter or one lowercase letter, or one character class.

You can use the **load-key-file** **URL filename** statement to load an SSH key file that was previously generated using **ssh-keygen**. The **URL filename** is the path to the file's location and name. When using this option, the contents of the key file are copied into the configuration immediately after entering the **load-key-file** **URL** statement. This command loads RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys.

Starting in Junos OS Release 18.3R1, the **ssh-dss** and **ssh-dsa** hostkey algorithms are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

Optionally, you can use the **ssh-dsa**, **ssh-ecdsa**, or **ssh-rsa** statements to directly configure SSH RSA, DSA, or ECDSA keys to authenticate root logins. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them.

```
[edit system]
user@host# set root-authentication load-key-file my-host:.ssh/id_dsa.pub
.file.19692 | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
[edit system]
```
From configuration mode, you can confirm your SSH key entries by entering the `show` command. It should look something like this:

```
[edit system]
user@hos# show
root-authentication {
    ssh-rsa "$ABC123"; # SECRET-DATA
}
```

Junos-FIPS software has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router or switch, you cannot configure passwords unless they meet this standard.

If you use the `encrypted-password` option, then a null-password (empty) is not permitted. You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

SEE ALSO

* Protecting Network Security by Configuring the Root Password
* Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

Example: Configuring a Plain-Text Password for Root Logins

This example shows how to configure a plain-text password for the root-level user (whose username is `root`). Configuring a plain-text password is one way to protect access to the root level by unauthorized
users. You must prevent unauthorized users from gaining access to superuser commands that can be used to alter your system configuration.

Requirements

No special configuration beyond device initialization is required before configuring this example.

Make sure that you understand the requirements for a valid plain-text password. For Junos OS, the default requirements for a plain-text password are as follows:

- Must be from 6 up to 128 characters long.
- Can include most character classes (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- Must contain at least one change of case or character class.

Overview

Junos OS is preinstalled on the router. When the router is powered on, it is ready to be configured. Initially, you log in as the root-level user with no password. To set the root password, you have several options. This example shows how to enter a plain-text password that Junos OS then encrypts for you.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following command and paste it into the window. When prompted, type the new password, and then when prompted, retype it.

```
set system root-authentication plain-text-password
```

Configuring a Plain-Text Password for User Root

Step-by-Step Procedure

To configure a plain-text password for the root-level user:

1. Type the `set` command for the plain-text password and press Enter.

```
[edit]
user@host# set system root-authentication plain-text-password
New password:
```

2. Type the new password next to the **New password** prompt and press Enter.
New password: **new-password**
Retype new password:

3. Retype the same password next to the **Retype new password** prompt and press Enter.

**Results**

From configuration mode, confirm your configuration by using the **show** command. It should look something like this:

```
[edit]
user@host# show system
root-authentication {
  encrypted-password "$ABC123"; ## SECRET-DATA
}
```

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

After you have confirmed that the configuration is correct, enter **commit** from configuration mode.

**Verification**

**Verifying the Configuration of a Plain-Text Password for User Root**

**Purpose**
Verify the configuration of a plain-text password for the root-level user.

**Action**
From operational mode, confirm your configuration by entering the **show configuration system** command.

```
user@host> show configuration system
root-authentication {
  encrypted-password "$ABC123"; ## SECRET-DATA
}
```

**Meaning**

If you use a clear-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see the unencrypted password. That is, as you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password as in some other systems. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.
Example: Configuring SSH Authentication for Root Logins

The following example shows how to configure two public DSA keys for SSH authentication of root logins:

```
[edit system]
root-authentication {
    encrypted-password "$ABC123";
    ## SECRET-DATA;
    ssh-dsa "2354 95 9304@user.device";
    ssh-dsa "0483 02 8362@user.device";
}
```

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3R1</td>
<td>Starting in Junos OS Release 18.3R1, the <code>ssh-dss</code> and <code>ssh-dsa</code> hostkey algorithms are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- *Protecting Network Security by Configuring the Root Password*
- *Plain-Text Passwords | 196*
- *Release Information for Junos OS with Upgraded FreeBSD*
Recovering Root Password

If you forget the root password for a device running Junos OS, you can use the password recovery procedure to reset the root password. Read this topic to understand how to recover root password.

Recovering the Root Password

If you forget the root password for the router, you can use the password recovery procedure to reset the root password.

Before you begin, note the following:

- You need console access to recover the root password.
- This password recovery procedure does not apply to devices running Junos OS with Upgraded FreeBSD. See "Recovering the Root Password on Junos OS with Upgraded FreeBSD" on page 186. For the list of Junos OS devices with upgraded FreeBSD, see Junos kernel upgrade to FreeBSD 10+.
- For MX80 Series routers, try this procedure first, but if it does not work you can manually delete the root-authentication settings from the Junos configuration file and reset the password, as explained here: Recovering the Root Password for MX80

Video: Recovering the Root Password

To recover the root password:

1. Power off the router by pressing the power button on the front panel.

2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.
3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45–to–DB-9 serial port adapter supplied with the router.

4. Plug the RJ-45–to–DB-9 serial port adapter into the serial port on the management device.

5. Connect the other end of the Ethernet rollover cable to the console port on the router.

6. Turn on the power to the management device.

7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

9. Power on the router by pressing the power button on the front panel.
   Verify that the POWER LED on the front panel turns green.
   The terminal emulation screen on your management device displays the router’s boot sequence.

10. When the following prompt appears, press the Spacebar to access the router’s bootstrap loader command prompt:
    Depending on your device hardware, the bootstrap loader might proceed quite quickly at this step without pausing for input. Therefore, you might need to press the spacebar multiple times at the beginning of the boot sequence.

    Hit [Enter] to boot immediately, or space bar for command prompt.
    Booting [kernel] in 9 seconds...

11. At the following prompt, type `boot -s` to start the system in single-user mode.
    
    ok  boot -s

12. At the following prompt, type `recovery` to start the root password recovery procedure.
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery

13. Enter configuration mode in the CLI.

14. Set the root password.

[edit]
user@host# set system root-authentication plain-text-password

When you configure a plain-text password, Junos OS encrypts the password for you.

⚠️ CAUTION: Do not use the encrypted-password option unless the password is already encrypted, and you are entering the encrypted version of the password. If you commit the encrypted-password option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the device as root, and you will need to repeat this password recovery process.

15. At the following prompt, enter the new root password, for example:

New password: password

Retype new password:

16. At the second prompt, reenter the new root password.

17. After you have finished configuring the password, commit the configuration.

root@host# commit

commit complete

18. Exit configuration mode in the CLI.

19. Exit operational mode in the CLI.

20. At the prompt, type y to reboot the router.

Reboot the system? [y/n] y
Recovering the Root Password on Junos OS with Upgraded FreeBSD

If you forget the root password for a device running Junos OS with Upgraded FreeBSD, you can use the password recovery procedure to reset the root password.

For the list of Junos OS devices with upgraded FreeBSD, see Junos kernel upgrade to FreeBSD 10+

**NOTE:** You need console access to recover the root password.

**NOTE:** This password recovery procedure only applies to devices running Junos OS with Upgraded FreeBSD. For password recovery on Junos OS devices, see “Recovering the Root Password” on page 183.

To recover the root password:

1. Power off the router by pressing the power button on the front panel.

2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.

3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45–to–DB-9 serial port adapter supplied with the router.

4. Plug the RJ-45–to–DB-9 serial port adapter into the serial port on the management device.

5. Connect the other end of the Ethernet rollover cable to the console port on the router.

6. Turn on the power to the management device.

7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

9. Power on the router by pressing the power button on the front panel.
   Verify that the POWER LED on the front panel turns green.
   The terminal emulation screen on your management device displays the router's boot sequence.

10. Access the Junos Main Menu.
   - Prior to Junos OS Release 17.3, the Junos Main Menu appears for 3 seconds on startup before automatically booting the Junos volume. Press any key within the 3 second window to stop the automatic boot sequence and display the Junos Main Menu.

   **NOTE:** The Junos Main Menu will appear every time you reboot the router while connected to the console.

   - Starting in Junos OS Release 17.3, press Ctrl+c at the following part in the reboot to bring up the Junos Main Menu:

   FreeBSD/x86 bootstrap loader, Revision 1.1  
   (builder@feyrith.juniper.net, Sun Feb 4 13:06:24 PST 2018)
   /
   Autoboot in 1 seconds... (press Ctrl-C to interrupt)

   1. Boot [J]unos volume
   2. Boot Junos volume in [S]afe mode
   3. [R]eboot
   4. [B]oot menu
   5. [M]ore options

11. At the Junos Main Menu, press the M or 5 key to activate the 5. [M]ore options menu:
1. Recover [J]unos volume
2. Recovery mode - [C]LI
3. Check [F]ile system
4. Enable [V]erbose boot
5. [B]oot prompt
6. [M]ain menu

12. Press the C or 2 key to access the 2. **Recovery mode - [C]LI** option. The router will reboot into CLI recovery mode.

13. When prompted, press the Enter key to immediately boot the router, or press any other key to bring up the command prompt.

14. Enter configuration mode in the CLI.

```
root># configure
```

Entering configuration mode

15. Set the root password.

When you configure a plain-text password, Junos OS encrypts the password for you.

```
[edit]
root# set system root-authentication plain-text-password
```

**CAUTION:** Do not use the `encrypted-password` option unless the password is _already_ encrypted, and you are entering the encrypted version of the password. If you commit the `encrypted-password` option with a plain-text password or with blank quotation marks (" "), you will not be able to log in to the router as root, and you will need to repeat this password recovery process.

16. At the following prompt, enter the new root password, for example:

```
New password: password
```
17. At the second prompt, reenter the new root password.

Recovering the Root Password for Junos OS Evolved

This procedure resets the root password without resetting the device configuration to the factory default configuration. Only the root password is reset to a value you enter. None of the other functions nor the state of the device are affected.

Connecting to the Serial Port

The first task in the password reset operation is to connect to the serial port of the device.

To connect to the serial port:

1. Power off the router by pressing the power button on the front panel.

2. Turn off the power to the management device, such as a PC or laptop computer, that you want to use to access the CLI.

3. Plug one end of the Ethernet rollover cable supplied with the router into the RJ-45-to-DB-9 serial port adapter supplied with the router.

4. Plug the RJ-45-to-DB-9 serial port adapter into the serial port on the management device.

5. Connect the other end of the Ethernet rollover cable to the console port on the router.

6. Turn on the power to the management device.
7. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

8. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

9. Power on the router by pressing the power button on the front panel.

   Verify that the POWER LED on the front panel turns green. The terminal emulation screen on your management device displays the router’s boot sequence.
Recovering the Root Password

The password reset operation is triggered early in the boot process, The actual password reset is done in the shell.

To recover the root password for Junos OS Evolved:

1. Do a hard reboot of the Routing Engine (that is, reboot a device that is not running).

   On the terminal, you see this screen:

   ![GNU GRUB  version 2.02-beta3](image)

   Use the ^ and v keys to select which entry is highlighted.
   Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

2. Use the arrow keys to scroll down to the Primary [Recover password] option and press Enter.

   ![Disk boot ...](image)

   Disk boot ...
   IMA is 0
   Loading kernel ...ok.
   Loading initrd ...ok.
   Booting ...
   [ 0.791088] Failed to find cpu0 device node
   Processing /dev/sda2 for mount on /soft ...[checking]..ok [mounting]..done
   Processing /dev/sda5 for mount on /data ...[checking]..ok [mounting]..done
   Processing /dev/sda6 for mount on /data/config ...[checking]..ok [mounting]..done

   ![Loading kernel ...ok.](image)
   ![Loading initrd ...ok.](image)
Processing /dev/sda7 for mount on /data/var ... [checking]..ok [mounting]..done

mkswap: /dev/sda3: warning: wiping old swap signature.
Setting up swappingspace version 1, size = 4 GiB (4294963200 bytes)
no label, UUID=7d905478-773b-41e5-8f1d-8166ec03f93a

Processing /dev/sda1 for mount on /boot ... [checking]..ok [mounting]..done
Done with local filesystems setup.

Mounting version

junos-linux-install-px-x86-64-16.2I20180502181332_evo-builder... done.

System is running with minimal count of software versions

modprobe: FATAL: Module jnx Cbd_fpga_ptx21k not found in directory
/lib/modules/4.8.24-WR2.2.1_standard

Installing kexec kernel... Cannot get kernel page_offset_base symbol address
done

Password recovery in progress. Please enter new password.

3. Enter the new password, and then retype the new password and Enter.

    New password:
    Retype new password:
    passwd: password updated successfully
    Password recovery done

    Welcome to Linux!

The reboot will proceed until the login prompt is displayed.

    [ OK ] Started Serial Getty on ttyS0.
    [ OK ] Reached target Login Prompts.
    [ OK ] Started Vsftpd ftp daemon.
    [ OK ] Started strongSwan IPsec IKEv1/IKEv2 daemon using swanctl.
    [ OK ] Started Arp filtering arptables.
    [ OK ] Started Management Ethernet Interface Manager Service.
    [ OK ] Started OFP on RE.

    Starting MGD initialization of schema and database on RE...

    Juniper Linux Distribution 2.2.1 re0 ttyS0

    re0 login:

4. Enter your login ID, and then your password.

    You will see a shell prompt.
5. To start the CLI, enter `cli`.

## Troubleshooting Loss of the Root Password

**Problem**

**Description:** If you forget the root password for a switch, use the password recovery procedure to reset the root password.

**NOTE:** You need physical access to the switch to recover the root password.

**TIP:** For a video on recovering the root password for routers, see “Root Password” on page 177. The procedure is similar for switches.

**Solution**

To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.

2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 3 on page 194.
3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).

4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

   **NOTE:** On EX2300 and EX3400 switches after step 5, use the following procedure:

   In the main menu that appears, select [M]ore options > Recovery mode - [C]LI.

   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

   Proceed to Step 9 in this procedure.

6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt:

   *Hit [Enter] to boot immediately, or space bar for command prompt.*

   *Booting [kernel] in 1 second...*
NOTE: If the switch is in unattended mode for U-Boot, access to the bootstrap loader command prompt is blocked. If the root password is lost, you must reset the switch to the factory default configuration using the LCD panel. For more information, see Reverting to the Default Factory Configuration for the EX Series Switch.

7. At the following prompt, type `boot -s` to start up the system in single-user mode:
   
   `loader> boot -s`

8. At the following prompt, type `recovery` to start the root password recovery procedure:
   
   `Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery`
   
   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:
   
   `user@switch> configure`

10. Set the root password. For example:
    
    `user@switch# set system root-authentication plain-text-password`

11. At the following prompt, enter the new root password. For example, `juniper1`:
    
    `user@switch# juniper1`
    
    `Retype new password:`

12. At the second prompt, reenter the new root password.

13. If you are finished configuring the network, commit the configuration.
    
    `root@switch# commit`
    
    `commit complete`

14. Exit configuration mode in the CLI.
    
    `root@switch# exit`

15. Exit operational mode in the CLI.
16. At the prompt, enter `y` to reboot the switch.
    Reboot the system? [y/n] y

SEE ALSO

- Connecting and Configuring an EX Series Switch (CLI Procedure)
- Connecting and Configuring an EX Series Switch (J-Web Procedure)

Plain-Text Passwords

IN THIS SECTION

- Changing the Requirements for Junos OS Plain-Text Passwords | 196
- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

Changing the Requirements for Junos OS Plain-Text Passwords

For plain-text password requirements, see Special Requirements for Junos OS Plain-Text Passwords.

To change the requirements for plain-text passwords, include the `password` statement at the `[edit system login]` hierarchy level:

```
[edit system login]
pwd 
    change-type (set-transitions | character-set);
    format (sha1 | sha256 | sha512);
    maximum-length length;
    maximum-lifetime days
    minimum-changes number;
    minimum-character-changes number
    minimum-length length;
```
NOTE: These statements apply to plain-text passwords only, not encrypted passwords.

SEE ALSO

- Configuring the Root Password | 177
- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

Example: Changing the Requirements for Junos OS Plain-Text Passwords

This example shows how to set various maximum and minimum requirements for plain-text passwords to increase password strength.
Requirements

This example requires a device running Junos 12.2 or greater. The **minimum-length** and **maximum-length** password requirements statements are available in earlier releases, however, you must have Junos OS Release 12.2 or greater to configure **minimum-lower-cases**, **minimum-numerics**, **minimum-punctuations**, or **minimum-upper-cases**.

Overview

You can use a variety of requirements to strengthen plain-text passwords for greater security. Junos OS provides a number of possible configurations at the [edit system login password] hierarchy level that allow you to require users to create plain-text passwords that conform to a particular set of requirements that may include such things as length, number of changes, type of characters, numbers, or letter case.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set system login password minimum-length 12
set system login password maximum-length 22
set system login password minimum-numerics 1
set system login password minimum-upper-cases 1
set system login password minimum-lower-cases 1
set system login password minimum-punctuations 1
```

**Configuring Requirements for Plain-Text Passwords**

Step-by-Step Procedure

This example configures password requirements that require the user to create a password that has a minimum length of 12 characters, a maximum length of 22 characters, and that includes at least one lower-case letter, at least one upper-case letter, at least one punctuation character, and at least one numeric character.

1. Navigate to configuration mode in the [system login password] hierarchy level.

```
user@host> edit
[edit]
user@host# edit system login password
```
2. Set a minimum length requirement of 12 characters and a maximum length requirement of 22 characters for user passwords.

[edit system login password]
user@host# set minimum-length 12
[edit system login password]
user@host# set maximum-length 22

3. Require users to set a password that has at least one lower-case letter and at least one upper-case letter.

[edit system login password]
user@host# set minimum-lower-cases 1
[edit system login password]
user@host# set minimum-upper-cases 1

4. Require users to set a password that has at least one punctuation-class character and at least one number.

[edit system login password]
user@host# set minimum-punctuations 1
[edit system login password]
user@host# set minimum-numerics 1

**Results**

From configuration mode, confirm your configuration by entering the show command at the edit system login password hierarchy level. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[edit system login password]
user@host# show
minimum-length 12;
maximum-length 22;
minimum-numerics 1;
minimum-upper-cases 1;
minimum-lower-cases 1;

SEE ALSO
Junos OS supports encryption method for configuration secrets using a master password. The master password derives an encryption key that uses AES256-GCM to protect certain secrets such as private keys, system master passwords, and other sensitive data by storing it in an AES256 encrypted format. For more information, read this topic.

Understanding Hardening Shared Secrets

Existing shared secrets ($9$ format) in Junos OS currently use an obfuscation algorithm, which is not a very strong encryption for configuration secrets. If you want a strong encryption for your configuration secrets, you can configure a master password. The master password is used to derive an encryption key that is used with AES256-GCM to encrypt configuration secrets. This new encryption method uses the $8$ formatted strings.

Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets. The master password encrypts secrets like the RADIUS password, IKE preshared keys, and other shared secrets in the Junos OS.
management process (mgd) configuration. The master password itself is not saved as part of the configuration. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. The key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text). See Figure 4 on page 201

Figure 4: Master Password Encryption

![Diagram of Master Password Encryption]

The $8$ configuration secrets can only be shared between devices using the same master password.

The $8$-encrypted passwords have the following format:

$8$crypt-algo$hash-algo$iterations$salt$iv$tag$encrypted. See Table 11 on page 201 for the master password format details.

Table 11: $8$-encrypted Password Format

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypt-algo</td>
<td>Encryption/decryption algorithm to be used. Currently only AES256-GCM is supported.</td>
</tr>
<tr>
<td>hash-algo</td>
<td>Hash (prf) algorithm to be used for the PBKDF2 key derivation.</td>
</tr>
<tr>
<td>iterations</td>
<td>The number of iterations to use for the PBKDF2 hash function. Current iteration-count default is 100. The iteration count slows the hashing count, thus slowing attacker guesses.</td>
</tr>
<tr>
<td>salt</td>
<td>Sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used to salt (a random, but known string) the password and input to the PBKDF2 key derivation.</td>
</tr>
<tr>
<td>iv</td>
<td>A sequence of ASCII64-encoded pseudorandom bytes generated during encryption that are to be used as initialization vector for the AES256-GCM encryption function.</td>
</tr>
<tr>
<td>tag</td>
<td>ASCII64-encoded representation of the tag.</td>
</tr>
</tbody>
</table>
Table 11: $8$-encrypted Password Format (continued)

<table>
<thead>
<tr>
<th>encrypted</th>
<th>ASCII64-encoded representation of the encrypted password</th>
</tr>
</thead>
</table>

The ASCII64 encoding is Base64 (RFC 4648) compatible, except no padding (character "=") is used to keep the strings short. For example:

$8$ae5256-gcm$hmac-sha2-256$100$y/4YMC4YDLU$fzYDIjN6YCyQsYLsaf8A$llu4jLcZarD9YnyD /Hejww$okhBlc0cGakSqqYxKww

Chassis Cluster Considerations

When defining a chassis cluster on SRX Series devices, be aware of the following restrictions:

- For SRX Series devices, first configure the master password on each node, and then build the cluster. The same master password should be configured on each node.
- In chassis cluster mode, the master password cannot be deleted.

NOTE: A change in the master password would mean disruption in chassis clustering; therefore you must change the password on both nodes independently.

Using Trusted Platform Module to Bind Secrets on SRX Series Devices

By enabling the Trusted Platform Module (TPM) on the SRX Series devices, the software layer leverages the use of the underlying TPM chip. TPM is a specialized chip that protects certain secrets at rest such as private keys, system master passwords, and other sensitive data by storing it in an AES256 encrypted format (instead of storing sensitive data in a clear text format). The device also generates a new SHA256 hash of the configuration each time the administrator commits the configuration. This hash is verified each time the system boots up. If the configuration has been tampered with, the verification fails and the device
will not continue to boot. Both the encrypted data and the hash of the configuration is protected by the TPM module using the master encryption password.

**NOTE:** Hash validation is performed during any commit operation by performing a validation check of the configuration file against the saved hash from previous commits. In a chassis cluster system, hash is independently generated on the backup system as part of the commit process. A commit from any mode, that is, batch-config, dynamic-config, exclusive-config, or private config generates the integrity hash.

**NOTE:** Hash is saved only for the current configuration and not for any rollback configurations. Hash is not generated during reboot or shutdown of the device.

The TPM encrypts the following secrets:

- SHA256 hash of the configuration
- device master-password
- all key-pairs on the device

The TPM chip is available on the SRX300, SRX320, SRX340, and SRX345 devices. TPM is not enabled by default. To enable TPM, see "Enabling the TPM" on page 204.

**Limitations**

The following limitations and exceptions apply to the configuration file integrity feature using TPM:

- This feature is supported only on the SRX300, SRX320, SRX340 and SRX345 devices.
- If the master encryption password is not set, data is stored unencrypted.
- If the master encryption password and the multiple index backup files are deleted, data cannot be decrypted.
- If you set up the master encryption password, downgrading to older releases that do not implement TPM is not supported. You must delete the master encryption password and reenter all sensitive data before downgrading.
- If the master encryption password was deleted before the daemons had a chance to re-encrypt the data, then the data becomes unusable.
- The file integrity feature is not supported along with the configuration file encryption feature that uses keys saved in EEPROM. You can enable only one function at a time.
Enabling the TPM

NOTE: Before enabling TPM, ensure that you have configured "set system master-password plain-text-password" otherwise, certain sensitive data will not be protected by the TPM.

You can enable the TPM by setting the master encryption password using the following CLI command:

request security tpm master-encryption-password set plain-text-password

You will be prompted to enter the master encryption password twice, to make sure that these passwords match. The master encryption password is validated for required password strength.

After master encryption password is set, the system proceeds to encrypt the sensitive data with the master encryption password which is encrypted by the Master Binding Key that is owned and protected by the TPM chip.

NOTE: If there is any issue with setting the master encryption password, a critical ERROR message is logged on the console and the process is aborted.

Verifying the Status of the TPM

You can use the show security tpm status command to verify the status of the TPM. The following information is displayed:

- TPM enabled/disabled
- TPM ownership
- TPM’s Master Binding Key status (created or not created)
- master encryption password status (set or not set)

Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices. To confirm the TPM firmware version, use the show security tpm status command. TPM Family and TPM Firmware version output fields are introduced.

Changing the Master Encryption Password

Changing the master encryption password is done using the CLI.
To change the master encryption password, enter the following command from operational mode:

```
request security tpm master-encryption-password set plain-text-password
```

**NOTE:** It is recommended that no configuration changes are made while you are changing the master encryption password.

The system checks if the master encryption password is already configured. If master encryption password is configured, then you are prompted to enter the current master encryption password.

The entered master encryption password is validated against the current master encryption password to make sure these master encryption passwords match. If the validation succeeds, you will be prompted to enter the new master encryption password as plain text. You will be asked to enter the key twice to validate the password.

The system then proceeds to re-encrypt the sensitive data with the new master encryption password. You must wait for this process of re-encryption to complete before attempting to change the master encryption password again.

If for some reason, the encrypted master encryption password file is lost or corrupted, the system will not be able to decrypt the sensitive data. The system can only be recovered by re-importing the sensitive data in clear text, and re-encrypting them.

If the system is compromised, the administrator can recover the system using one of the following methods:

- Clear the TPM ownership in u-boot and then install the image in boot loader using TFTP or USB (if USB port is not restricted).

**NOTE:** If the installed software version is older than Junos OS Release 15.1X49-D110 and the master encryption password is enabled, then installation of Junos OS Release 15.1X49-D110 will fail. You must backup the configuration, certificates, key-pairs, and other secrets and use the TFTP/USB installation procedure.
Starting with Junos OS Release 15.1X49-D120 and Junos OS Release 17.4R1, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see [Upgrading TPM Firmware on SRX-Devices](#). To confirm the TPM firmware version, use the `show security tpm status` command. **TPM Family** and **TPM Firmware version** output fields are introduced.

Starting with Junos OS Release 15.1X49-D50, new CLI commands are introduced to configure a system master password to provide stronger encryption for configuration secrets.

### RELATED DOCUMENTATION

- **master-password**: 1936
- **Root Password**: 177
- **Plain-Text Passwords**: 196
User Authentication

Junos OS User Authentication Overview | 209
Authentication Order for RADIUS, TACACS+, and Local Password | 218
RADIUS Authentication | 233
RADIUS over TLS (RADSEC) | 259
TACACS+ Authentication | 263
Authentication for Routing Protocols | 283
Junos OS User Authentication Overview

Junos OS supports different methods such as local password authentication, RADIUS and TACACS+ to control access to the network. Authentication methods are used for validating users who attempt to access the router or switch using telnet. Authentication prevents unauthorized devices and users from gaining access to your LAN. For more information, read this topic.

Junos OS User Authentication Methods

The Junos OS supports three methods of user authentication: local password authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+).

With local password authentication, you configure a password for each user allowed to log in to the router or switch.

RADIUS and TACACS+ are authentication methods for validating users who attempt to access the router or switch using telnet. They are both distributed client-server systems—the RADIUS and TACACS+ clients run on the router or switch, and the server runs on a remote network system.

You can configure the router or switch to be both a RADIUS and TACACS+ client, and you can also configure authentication passwords in the Junos OS configuration file. You can prioritize the methods to configure the order in which the software tries the different authentication methods when verifying user access.

You can control access to your network using several different authentication methods—media access control (MAC) RADIUS, for example. Authentication prevents unauthorized devices and users from gaining access to your LAN. For MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a DHCP server.
NOTE: Note about the MAC RADIUS authentication:

- You can enable end devices to access the network without authenticating on the RADIUS server by configuring the MAC address of the end device in the static MAC bypass list by configuring the MAC address using the `authentication-whitelist` statement.

- You can configure one or more authentication methods on a single interface and thereby enable fallback to the next method if the first or second method is unsuccessful.

- On a single interface you can configure one or a combination of several authentication methods.

- The EAP method supported for MAC RADIUS authentication is EAP-MD5.

- You can configure MAC RADIUS authentication on interfaces that are connected to end devices.

- When you configure the `mac-radius restrict` option, the switch immediately attempts a MAC-RADIUS authentication by sending a request to the RADIUS server for authentication of the MAC address of the end device. If MAC address of the end device is configured for RADIUS authentication, LAN access between the two switches is created.

SEE ALSO

- Configuring RADIUS Server Authentication | 233
- Configuring TACACS+ Authentication | 264
- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication | 218

### Configuring Local User Template Accounts for User Authentication

You use local user template accounts when you need different types of templates for authentication. Each template can define a different set of permissions appropriate for the group of users who use that template. These templates are defined locally on the router or switch and referenced by the TACACS+ and RADIUS authentication servers.

When you configure local user templates and a user logs in, Junos OS issues a request to the authentication server to authenticate the user’s login name. If a user is authenticated, the server returns the local username to Junos OS, which then determines whether a local username is specified for that login name (local-username for TACACS+, Juniper-Local-User for RADIUS). If so, Junos OS selects the appropriate local user template locally configured on the router or switch. If a local user template does not exist for the authenticated user, the router or switch defaults to the `remote` template.
To configure different access privileges for users who share the local user template account, include the `allow-commands` and `deny-commands` commands in the authentication server configuration file.

To configure a local user template, include the `user local-username` statement at the `[edit system login]` hierarchy level and specify the privileges you want to grant to the local users to whom the template applies:

```
[edit system login]
user local-username {
    full-name "Local user account";
    uid uid-value;
    class class-name;
}
```

This example configures the `sales` and `engineering` local user templates:

```
[edit]
system {
    login {
        user sales {
            uid uid-value;
            class class-name;
        }
        user engineering {
            uid uid-value;
            class class-name;
        }
    }
}
```

```
user = simon {
    ...
    service = junos-exec {
        local-user-name = sales
        allow-commands = "configure"
        deny-commands = "shutdown"
    }
}
user = rob {
    ...
    service = junos-exec {
        local-user-name = sales
        allow-commands = "(request system) | (show rip neighbor)"
        deny-commands = "clear"
    }
}
When the login users Simon and Rob are authenticated, the router or switch applies the sales local user template. When login users Harold and Jim are authenticated, the router or switch applies the engineering local user template.

SEE ALSO

| Example: Configuring Authentication Order | 227 |
| user (Access) | 2402 |

Configuring Remote Template Accounts for User Authentication

By default, the Junos OS uses remote template accounts for user authentication when:

- The authenticated user does not exist locally on the router or switch.
- The authenticated user’s record in the authentication server specifies local user, or the specified local user does not exist locally on the router or switch.

To configure the remote template account, include the `user remote` statement at the `[edit system login]` hierarchy level and specify the privileges you want to grant to remote users:
[edit system login]
user remote {
    full-name "All remote users";
    uid uid-value;
    class class-name;
}

To configure different access privileges for users who share the remote template account, include the \texttt{allow-commands} and \texttt{deny-commands} statements in the authentication server configuration file.

\textbf{SEE ALSO}

| Example: Configuring Authentication Order | 227 |
| user (Access) | 2402 |

\textbf{Example: Creating Template Accounts}

\textbf{IN THIS SECTION}

- Requirements | 213
- Overview | 214
- Configuration | 214
- Verification | 216

This example shows how to create template accounts.

\textbf{Requirements}

No special configuration beyond device initialization is required before configuring this feature.
Overview

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

By default, Junos OS uses the remote template account when:

- The authenticated user does not exist locally on the device.
- The authenticated user’s record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

In this example, you create a remote template account and set the username to remote and the login class for the user as operator. You create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

You then create a local template account and set the username as admin and the login class as superuser. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

Configuration

Creating a Remote Template Account

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system login user remote class operator
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To create a remote template account:

- Set the username and the login class for the user.

```
[edit system login]
user@host# set user remote class operator
```

**Results**

From configuration mode, confirm your configuration by entering the `show system login` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system login
user remote {
    class operator;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

**Creating a Local Template Account**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

```
set system login user admin class superuser
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To create a local template account:

1. Set the username and the login class for the user.

```
[edit system login]
user@host# set user admin class superuser
```
Results
From configuration mode, confirm your configuration by entering the **show system login** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
  user@host# show system login
  user admin {
    class super-user;
  }
```

If you are done configuring the device, enter **commit** from configuration mode.

**NOTE:** To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and specify a system authentication order. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 239.
- Configure system authentication order. See "Example: Configuring Authentication Order" on page 227.

Verification

Confirm that the configuration is working properly.

**Verifying the Template Accounts Creation**

**Purpose**
Verify that the template accounts have been created.

**Action**
From operational mode, enter the **show system login** command.

SEE ALSO

Junos OS User Accounts Overview | 91
Understanding Remote Authentication Servers

You probably already use a remote authentication server (or servers) in your network. It is a recommended best practice, because the servers allow you to centrally create a consistent set of user accounts for all devices in your network. There are many good reasons for implementing a authentication, authorization, and accountability (AAA) solution in your network, not the least of which is to make the management of user accounts easier.

There are two basic methods of remote authentication in use by most enterprises today—RADIUS and TACACS+. Junos OS supports both types and can be configured to query multiple remote authentication servers of both types. The idea behind a RADIUS or TACACS+ server is simple, a central authentication server that routers, switches, security devices, and even servers can use to authenticate users as they attempt to gain access to these systems. Think of the advantages that a central user directory brings for authentication auditing and access control in a client server model, and you have your justification for RADIUS or TACACS+ for your networks infrastructure.

Using a central server has multiple advantages over the alternative of creating local users on each device, a time-consuming and error-prone task. A central authentication system also simplifies the use of one-time password systems such as SecureID, which offer protection against password sniffing and password replay attacks, in which someone uses a captured password to pose as a system administrator.

- **RADIUS**—You should use RADIUS when your priorities are interoperability and performance.
  - Interoperability—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
  - Performance—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.

- **TACACS+**—You should use TACACS+ when your priorities are security and flexibility.
  - Security—TACACS+ is more secure than RADIUS. Not only is the full session encrypted, but authorization and authentication are done separately to prevent someone from trying to force their way into your network.
  - Flexibility—TCP is a more flexible transport protocol than UDP. You can do more with it in more advanced networks. In addition, TACACS+ supports more of the enterprise protocols like NetBios or Appletalk.

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Authentication Order for RADIUS, TACACS+, and Local Password</th>
<th>218</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Authentication</td>
<td>233</td>
</tr>
</tbody>
</table>
Authentication Order for RADIUS, TACACS+, and Local Password

IN THIS SECTION

- Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication | 218
- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication | 225
- Example: Configuring Authentication Order | 227
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication | 230

Junos OS supports different methods such as local password authentication, RADIUS and TACACS+ to control access to the network. Authentication methods are used for validating users who attempt to access the router or switch using telnet. You can prioritize the methods to configure the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch or security device. For more information, read this topic.

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication

Using the `authentication-order` statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch.

If RADIUS and/or TACACS+ servers are configured in the authentication order but there is no response from them to a request, the Junos OS always defaults to trying local password authentication as a last resort. If the authentication order is set to `authentication-order password`, that will be the only authentication method attempted.
NOTE: It is not possible and would make no sense to try to configure local password authentication ahead of RADIUS or TACACS+ in the order because "no response" cannot happen. A local authentication request will always either be accepted or rejected.

The handling of a rejected authentication request when RADIUS or TACACS+ are present is more complicated.

- If **password** (local password authentication) is *not* in the authentication order, a RADIUS and/or TACACS+ rejection ends with the rejection.
- If **password** is included at the end of the authentication order and RADIUS and/or TACACS+ rejects the authentication, the Junos OS tries for a local authentication check.

In other words, including **password** as a final authentication order option is a means by which you can choose whether a RADIUS and/or TACACS+ rejection ends there or if the request is to be given one last chance for authentication locally.

**Using RADIUS or TACACS+ Authentication**

You can configure the Junos OS to be both a RADIUS and TACACS+ authentication client.

If an authentication method included in the `[authentication-order]` statement is not available, or if the authentication is available but returns a reject response, the Junos OS tries the next authentication method included in the `authentication-order` statement.

The RADIUS or TACACS+ server authentication might fail because of the following reasons:

- The authentication method is configured, but the corresponding authentication servers are not configured. For instance, the RADIUS and TACACS+ authentication methods are included in the `authentication-order` statement, but the corresponding RADIUS or TACACS+ servers are not configured at the respective `[edit system radius-server]` and `[edit system tacplus-server]` hierarchy levels.
- The RADIUS or TACACS+ server does not respond within the timeout period configured at the `[edit system radius-server]` or `[edit system tacplus-server]` hierarchy levels.
- The RADIUS or TACACS+ server is not reachable because of a network problem.

The RADIUS or TACACS+ server authentication might return a reject response because of the following reasons:

- The user profiles of users accessing a router or switch might not be configured on the RADIUS or TACACS+ server.
- The user enters incorrect logon credentials.
Using Local Password Authentication

You can explicitly configure the password authentication method or use this method as a fallback mechanism when remote authentication servers fail. The password authentication method consults the local user profiles configured at the [edit system login] hierarchy level. Users can log in to a router or switch using their local username and password in the following scenarios:

- The password authentication method (password) is explicitly configured as one of the authentication methods in the [authentication-order authentication-methods] statement. In this case, the password authentication method is tried if no previous authentication accepts the logon credentials. This is true whether the previous authentication method fails to respond or returns a reject response because of an incorrect username or password.

- The password authentication method is not explicitly configured as one of the authentication methods in the [authentication-order authentication-methods] statement. In this case, the password authentication method is tried only if all configured authentication methods fail to respond. It is not consulted if any configured authentication method returns a reject response because of an incorrect username or password.

Order of Authentication Attempts

Table 12 on page 220 describes how the authentication-order statement at the [edit system] hierarchy level determines the procedure that the Junos OS uses to authenticate users for access to a router or switch.

Table 12: Order of Authentication Attempts

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Order of Authentication Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-order radius;</td>
<td>1. Try configured RADIUS authentication servers.</td>
</tr>
<tr>
<td></td>
<td>2. If RADIUS server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>3. If RADIUS server is available but authentication is rejected, deny access.</td>
</tr>
<tr>
<td></td>
<td>4. If RADIUS servers are not available, try password authentication.</td>
</tr>
<tr>
<td></td>
<td>NOTE: If a RADIUS server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</td>
</tr>
</tbody>
</table>
Table 12: Order of Authentication Attempts (continued)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Order of Authentication Attempts</th>
</tr>
</thead>
</table>
| authentication-order [ radius password ]; | 1. Try configured RADIUS authentication servers.  
2. If RADIUS servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order. |
| authentication-order [ radius tacplus ];  | 1. Try configured RADIUS authentication servers.  
2. If RADIUS server is available and authentication is accepted, grant access.  
3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.  
4. If TACACS+ server is available and authentication is accepted, grant access.  
5. If TACACS+ server is available but authentication is rejected, deny access.  
6. If both RADIUS and TACACS+ servers are not available, try password authentication.  
   NOTE: If either RADIUS or TACACS+ servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |
Table 12: Order of Authentication Attempts (continued)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Order of Authentication Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication-order [ radius tacplus password ];</strong></td>
<td>1. Try configured RADIUS authentication servers.</td>
</tr>
<tr>
<td></td>
<td>2. If RADIUS server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>3. If RADIUS servers fail to respond or return a reject response, try configured TACACS+ servers.</td>
</tr>
<tr>
<td></td>
<td>4. If TACACS+ server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>5. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</td>
</tr>
<tr>
<td><strong>authentication-order tacplus;</strong></td>
<td>1. Try configured TACACS+ authentication servers.</td>
</tr>
<tr>
<td></td>
<td>2. If TACACS+ server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>3. If TACACS+ server is available but authentication is rejected, deny access.</td>
</tr>
<tr>
<td></td>
<td>4. If TACACS+ servers are not available, try password authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If a TACACS+ server is available, password authentication is not attempted, because it is not explicitly configured in the authentication order.</td>
</tr>
<tr>
<td><strong>authentication-order [ tacplus password ];</strong></td>
<td>1. Try configured TACACS+ authentication servers.</td>
</tr>
<tr>
<td></td>
<td>2. If TACACS+ servers fail to respond or return a reject response, try password authentication, because it is explicitly configured in the authentication order.</td>
</tr>
</tbody>
</table>
Table 12: Order of Authentication Attempts (continued)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Order of Authentication Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication-order [ tacplus radius ];</strong></td>
<td>1. Try configured TACACS+ authentication servers.</td>
</tr>
<tr>
<td></td>
<td>2. If TACACS+ server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers.</td>
</tr>
<tr>
<td></td>
<td>4. If RADIUS server is available and authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>5. If RADIUS server is available but authentication is rejected, deny access.</td>
</tr>
</tbody>
</table>
| | 6. If both TACACS+ and RADIUS servers are not available, try password authentication.  
**NOTE:** If either TACACS+ or RADIUS servers are available, password authentication is not attempted, because it is not explicitly configured in the authentication order. |

| **authentication-order [ tacplus radius password ];** | 1. Try configured TACACS+ authentication servers. |
| | 2. If TACACS+ server is available and authentication is accepted, grant access. |
| | 3. If TACACS+ servers fail to respond or return a reject response, try configured RADIUS servers. |
| | 4. If RADIUS server is available and authentication is accepted, grant access. |
| | 5. If RADIUS servers fail to respond or return a reject response try password authentication, because it is explicitly configured in the authentication order. |
Table 12: Order of Authentication Attempts (continued)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Order of Authentication Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-order password;</td>
<td>1. Try to authenticate the user, using the password configured at the [edit system login] hierarchy level.</td>
</tr>
<tr>
<td></td>
<td>2. If the authentication is accepted, grant access.</td>
</tr>
<tr>
<td></td>
<td>3. If the authentication is rejected, deny access.</td>
</tr>
</tbody>
</table>

NOTE: If SSH public keys are configured, SSH user authentication first tries to perform public key authentication before using the authentication methods configured in the authentication-order statement. If you want SSH logins to use the authentication methods configured in the authentication-order statement without first trying to perform public key authentication, do not configure SSH public keys.

In a routing matrix based on a TX Matrix router, the authentication order must be configured only at the configuration groups re0 and re1. The authentication order must not be configured at the [edit system] hierarchy. This is because the authentication order for the routing matrix is controlled on the switch-card chassis (or TX Matrix router) or switch-fabric chassis (for TX Matrix Plus router) only.

In Junos OS Release 10.0 and later, the superuser (belonging to the super-user login class) is also authenticated based on the authentication order that is configured for TACACS+, RADIUS, or password authentication using the authentication-order statement. For example, if the only configured authentication order is TACACS+, the superuser can only be authenticated by the TACACS+ server and password authentication cannot be used as an alternative. However, in Junos OS Release 9.6 and earlier, the superuser can use password authentication to login, even if password authentication is not configured explicitly using the authentication-order statement.

SEE ALSO

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions  | 82
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication  | 230
Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication

Using the `authentication-order` statement, you can prioritize the order in which the Junos OS tries the different authentication methods when verifying user access to a router or switch. If you do not set the authentication order, by default users are verified based on their configured passwords.

When configuring a password using plain text and relying on Junos OS to encrypt it, you are still sending the password over the internet in plain text. Using pre-encrypted passwords is more secure because it means that the plain text of the password never has to be sent over the internet. Also, with passwords, only one user can be assigned to a password at a time.

On the other hand, both RADIUS and TACACS+ pre-encrypt passwords. Both let you assign a set of users at a time instead of one by one. But here are how these authentication systems differ:

- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS encrypts only the password during transmission whereas TACACS+ encrypts the entire session.
- RADIUS combines authentication (device) and authorization (user) whereas TACACS+ separates authentication, authorization, and accountability.

In short, TACACAS+ is the more secure of the two. However, RADIUS has better performance and is more interoperable. RADIUS is widely supported, whereas TACACS+ is a Cisco proprietary product and not widely supported outside of Cisco.

You can configure the authentication order based on your system, its restrictions, and your IT policy and operational preferences.

To configure the authentication order, include the `authentication-order` statement at the `[edit system]` hierarchy level:

```
[edit system]
    authentication-order [ authentication-methods ];
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.
Following are the possible authentication order entry options:

- **radius**—Verify the user using RADIUS authentication servers.
- **tacplus**—Verify the user using TACACS+ authentication servers.
- **password**—Verify the user using the username and password configured locally by including the authentication statement at the [edit system login user] hierarchy level.

If RADIUS and/or TACACS+ servers are configured in the authentication order but there is no response from them to a request, the Junos OS always defaults to trying local password authentication as a last resort. If the authentication order is set to **authentication-order password**, that will be the only authentication method attempted.

**NOTE:** It is not possible and would make no sense to try to configure local password authentication ahead of RADIUS or TACACS+ in the order because "no response" cannot happen. A local authentication request will always either be accepted or rejected.

The handling of a rejected authentication request when RADIUS or TACACS+ are present is more complicated.

- If **password** (local password authentication) is not in the authentication order, a RADIUS and/or TACACS+ rejection ends with the rejection.
- If **password** is included at the end of the authentication order and RADIUS and/or TACACS+ rejects the authentication, the Junos OS tries for a local authentication check.

In other words, including **password** as a final authentication order option is a means by which you can choose whether a RADIUS and/or TACACS+ rejection ends there or if the request is to be given one last chance for authentication locally.

For more details, see “Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication” on page 218.

The CHAP authentication sequence cannot take more than 30 seconds. If it takes longer to authenticate a client, the authentication is abandoned and a new sequence is initiated.

For example, if you configure three RADIUS servers so that the router or switch attempts to contact each server three times, and with each retry the server times out after 3 seconds, then the maximum time given to the RADIUS authentication method before CHAP considers it a failure is 27 seconds. If you add more RADIUS servers to this configuration, they might not be contacted because the authentication process might be abandoned before these servers are tried.

The Junos OS enforces a limit on the number of standing authentication server requests that the CHAP authentication can have at one time. Thus, an authentication server method—RADIUS, for example—might fail to authenticate a client when this limit is exceeded. If it fails, the authentication sequence is reinitiated
by the router or switch until authentication succeeds and the link is brought up. However, if the RADIUS servers are not available and if additional authentication methods such as tacplus or password are configured along with radius, the next authentication method is tried.

The following example shows how to configure radius and password authentication:

```
[edit system]
user@switch# authentication-order [ radius password ];
```

The following example shows how to delete the radius statement from the authentication order:

```
[edit system]
user@switch# delete authentication-order radius
```

The following example shows how to insert the tacplus statement after the radius statement:

```
[edit system]
user@switch# insert authentication-order tacplus after radius
```

SEE ALSO

- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands | 273
- authentication-order | 1518

**Example: Configuring Authentication Order**

This example shows how to configure authentication order.
Requirements

Before you begin, perform the initial device configuration. See the Getting Started Guide for your device.

Overview

You can configure the authentication methods that the device uses to verify that a user can gain access. For each login attempt, the device tries the authentication methods in order, starting with the first one, until the password matches. If you do not configure system authentication, users are verified based on their configured local passwords.

This example configures the device to attempt user authentication with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

When you use local password authentication, you must create a local user account for every user who wants to access the system. However, when you are using RADIUS or TACACS+ authentication, you can create single accounts (for authorization purposes) that are shared by a set of users. You create these accounts using the remote and local user template accounts. When a user is using a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective user ID are inherited from the template account.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
insert system authentication-order radius after password
insert system authentication-order tacplus after radius
```

GUI Step-by-Step Procedure

To configure authentication order:

1. In the J-Web user interface, select Configure>System Properties>User Management.

2. Click Edit. The Edit User Management dialog box appears.

3. Select the Authentication Method and Order tab.

4. Under Available Methods, select the authentication method the device should use to authenticate users, and use the arrow button to move the item to the Selected Methods list. Available methods include:
• RADIUS
• TACACS+
• Local Password

If you want to use multiple methods to authenticate users, repeat this step to add the additional methods to the Selected Methods list.

5. Under Selected Methods, use the Up Arrow and Down Arrow to specify the order in which the device should execute the authentication methods.

6. Click OK to check your configuration and save it as a candidate configuration.

7. If you are done configuring the device, click Commit Options>Commit.

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure authentication order:

1. Add RADIUS authentication to the authentication order.

   ```
   [edit]
   user@host# insert system authentication-order radius after password
   ```

2. Add TACACS+ authentication to the authentication order.

   ```
   [edit]
   user@host# insert system authentication-order tacplus after radius
   ```

Results
From configuration mode, confirm your configuration by entering the show system authentication-order command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   ```
   [edit]
   user@host# show system authentication-order
   authentication-order [password, radius, tacplus];
   ```

If you are done configuring the device, enter commit from configuration mode.
NOTE: To completely set up RADIUS or TACACS+ authentication, you must configure at least one RADIUS or TACACS+ server and create user template accounts. Do one of the following tasks:

- Configure a RADIUS server. See "Example: Configuring a RADIUS Server for System Authentication" on page 239.
- Configure a user. See "Example: Configuring New Users" on page 95.
- Configure template accounts. See "Example: Creating Template Accounts" on page 213.

Verification

Confirm that the configuration is working properly.

**Verifying the Authentication Order Configuration**

**Purpose**
Verify that the authentication order has been configured.

**Action**
From operational mode, enter the `show system authentication-order` command.

SEE ALSO

- Junos OS User Accounts Overview | 91
- Junos OS User Authentication Methods | 209

---

**Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication**

The following example shows how to configure system authentication for RADIUS, TACACS+, and password authentication.

In this example, only the user Philip and users authenticated by a remote RADIUS server can log in. If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the router or switch. If the RADIUS server is not available, the user is authenticated using the **password** authentication
method and allowed access to the router or switch. For more information about the password authentication method, see "Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication" on page 218.

When Philip tries to log in to the system, if the RADIUS server authenticates him, he is given access and privileges for the **super-user** class. Local accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same user ID (UID) 9999 and the privileges associated with the **operator** class.

```
[edit]
  system {
    authentication-order radius;
    login {
      user philip {
        full-name "Philip";
        uid 1001;
        class super-user;
      }
      user remote {
        full-name "All remote users";
        uid 9999;
        class operator;
      }
    }
  }
```

**NOTE:** For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time. For example, when you create a remote template account, a set of remote users can concurrently share a single UID. For more information about template accounts, see “Example: Configuring Authentication Order” on page 227.

When a user logs in to a device, the user’s login name is used by the RADIUS or TACACS+ server for authentication. If the user is authenticated successfully by the authentication server and the user is not configured at the [edit system login user] hierarchy level, the device uses the default remote template user account for the user, provided a remote template account is configured at the edit system login user remote hierarchy level. The remote template account serves as a default template user account for all users that are authenticated by the authentication server but not having a locally configured user account on the device. Such users share the same login class and UID.

To configure an alternate template user, specify the **user-name** parameter returned in the RADIUS authentication response packet. Not all RADIUS servers allow you to change this parameter. The following shows a sample Junos OS configuration:
Assume your RADIUS server is configured with the following information:

- User Philip with password "olympia"
- User Alexander with password "bucephalus" and username "operator"
- User Darius with password "redhead" and username "operator"
- User Roxane with password "athena"

Philip would be given access as a superuser (super-user) because he has his own local user account. Alexander and Darius share UID 9990 and have access as operators. Roxane has no template-user override, so she shares access with all the other remote users, getting read-only access.

SEE ALSO

Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication | 225

RELATED DOCUMENTATION
RADIUS Authentication

The Junos OS supports RADIUS for central authentication of users on multiple routers or switches or security devices. To use RADIUS authentication on the device, you must configure information about one or more RADIUS servers on the network. You can also configure RADIUS accounting on the device to collect statistical data about the users logging in to or out from a LAN and sending the data to a RADIUS accounting server. For more information, read this topic.

Configuring RADIUS Server Authentication

IN THIS SECTION

- Why Use RADIUS | 234
- Configuring RADIUS Server Details | 234
- Configuring RADIUS To Use the Management Instance | 238
RADIUS authentication is a method of authenticating users who attempt to access the router or switch.

Why Use RADIUS

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

You should use RADIUS when your priorities are interoperability and performance:

- Interoperability—RADIUS is more interoperable than TACACS+, primarily because of the proprietary nature of TACACS+. While TACACS+ supports more protocols, RADIUS is universally supported.
- Performance—RADIUS is much lighter on your routers and switches and for this reason, network engineers generally prefer RADIUS over TACACS+.

Configuring RADIUS Server Details

To use RADIUS authentication on the device, configure information about one or more RADIUS servers on the network by including one radius-server statement at the [edit system] hierarchy level for each RADIUS server.

Because remote authentication is configured on multiple devices, it is commonly configured inside of a configuration group. As such, the steps shown here are in a configuration group called global. Using a configuration group is optional.

**NOTE:** The remote statement must always be lowercase.

**NOTE:** This feature is supported on SRX1500, SRX5400, SRX5600, and SRX5800 devices.
To configure authentication by a RADIUS server:

1. Add an IPv4 or IPv6 server address.
   • Configure an IPv4 source-address and server-address:

```
[edit groups global]
user@host# set system radius-server server-address source-address source-address
```

For example:

```
[edit groups global]
user@host# set system radius-server 192.168.17.28 source-address 192.168.17.1
```

• Configure an IPv6 source-address and server address:

```
[edit groups global system radius-server server-address]
user@host# set server-address secret "secretkey" source-address-inet6 source-address
```

For example:

```
[edit groups global system radius-server ::17.22.22.162]
user@host# set secret $9$IPoV87ZGiH.5JGn/AtOB7-dVgo source-address-inet6 ::17.22.22.1
```

Source address is a valid IPv4 or IPv6 address configured on one of the router or switch interfaces. This sets a fixed address as the source address for locally generated IP packets.

Server address is a unique IPv4 or IPv6 address that is assigned to a particular server and used to route information to the server. If the Junos OS device has several interfaces that can reach the RADIUS server, assign an IP address that Junos OS can use for all its communication with the RADIUS server.

2. Include a shared secret password.

You must specify a password in the `secret password` statement. If the password contains spaces, enclose it in quotation marks. The secret password used by the local router or switch must match that used by the server. The secret password configures the password that the Junos OS device uses to access the RADIUS server.

```
[edit groups global system radius-server server-address]
user@host# set secret password
```
For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set secret $9$gQ4UHf5F36CiH.5Tc9CuO1hexm8xw2olENVwGZG
```

3. If necessary, specify a port on which to contact the RADIUS server.

By default, port number 1812 is used (as specified in RFC 2865).

**NOTE:** You can also specify an accounting port to send accounting packets with the `accounting-port` statement. The default is 1813 (as specified in RFC 2866).

```
[edit groups global system radius-server server-address]
user@host# set port port-number
```

For example:

```
[edit groups global system radius-server 192.168.69.162]
user@host# set port 1845
```

4. Specify the order in which Junos OS attempts authentication.

You must include the `authentication-order` statement in your remote authentication configuration.

The example assumes your network includes both RADIUS and TACACS+ servers. In this example, whenever a user attempts to log in, Junos OS begins by querying the RADIUS server for authentication. If it fails, it next attempts authentication with locally configured user accounts. Finally the TACACS+ server is tried.

```
[edit groups global system]
user@host# set authentication-order [ authentication-methods ]
```

For example:

```
[edit groups global system]
user@host# set authentication-order [ radius password tacplus ]
```

5. Assign a login class to RADIUS-authenticated users.
You can assign different user templates and login classes to RADIUS-authenticated users. This allows RADIUS-authenticated users to be granted different administrative permissions on the Junos OS device. By default, RADIUS-authenticated users use the `remote` user template and are assigned to the associated class, which is specified in the `remote` user template, if the `remote` user template is configured. The username `remote` is a special case in Junos OS. It acts as a template for users who are authenticated by a remote server, but do not have a locally configured user account on the device. In this method, Junos OS applies the permissions of the remote template to those authenticated users without a locally defined account. All users mapped to the remote template are of the same login class.

In the Junos OS configuration, a user template is configured in the same way as a regular local user account, except that no local authentication password is configured because the authentication is remotely performed on the RADIUS server.

- To use the same permissions for all RADIUS-authenticated users:

```
[edit groups global system login]
user@host# set user remote class class
```

For example:

```
[edit groups global system login]
user@host# set user remote class super-user
```

- To have different login classes be used for different RADIUS-authenticated users, granting them different permissions:

  a. Create multiple user templates in the Junos OS configuration.

        Every user template can be assigned a different login class.

        For example:

        ```
        [edit groups global system login]
        set user RO class read-only
        set user OP class operator
        set user SU class super-user
        set user remote full-name "default remote access user template"
        set user remote class read-only
        ```

  b. Have the RADIUS server specify the name of the user template to be applied to the authenticated user.

        For a RADIUS server to indicate which user template is to be applied, it needs to include the Juniper-Local-User-Name attribute (Vendor 2636, type 1, string) Juniper VSA (vendor-specific attribute) in the RADIUS Access-Accept message. The string value in the Juniper-Local-User-Name
must correspond to the name of a configured user template on the device. For a list of relevant
Juniper RADIUS VSAs, see "Juniper Networks Vendor-Specific RADIUS Attributes" on page 247.

If the Juniper-Local-User-Name is not included in the Access-Accept message or the string contains
a user template name that does not exist on the device, the user is assigned to the remote user
template, if configured. If it is not configured, authentication fails for the user.

After logging in, the remotely authenticated user retains the same username that was used to log
in. However, the user inherits the user class from the assigned user template.

In a RADIUS server, users can be assigned a Juniper-Local-User-Name string, which indicates the
user template to be used in the Junos OS device. From the previous example, the string would
be RO, OP, or SU. Configuration of the RADIUS server depends on the server being used.

Configuring RADIUS To Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for RADIUS through
the default routing instance. Starting in Junos OS Release 18.1R1, existing RADIUS behavior is enhanced
to support a management interface in a non-default VRF instance.

When the routing-instance mgmt_junos option is configured in both the radius-server server-ip-address
and the radius server server-ip-address statements, provided the management-instance statement is also
configured, RADIUS packets are routed through the management instance mgmt_junos.

```text
[edit system]
radius-server server-address {
    accounting-port port-number;
    port number;
    retry number;
    routing-instance routing-instance-name; #use "mgmt_junos" for RI name
    secret password;
    source-address source-address;
    timeout seconds;
}

[edit system accounting destination radius]
server {
    server-address {
        accounting-port port-number;
        retry number;
        routing-instance routing-instance; #use "mgmt_junos" for RI name
        secret password;
        source-address address;
        timeout seconds;
    }
```
NOTE: The routing-instance mgmt_junos option must be configured in both the radius-server and the radius server statements. If not, even if the management-instance statement is set, RADIUS packets will still be sent using the default routing instance only.

For more details on this management instance, see management-instance.

SEE ALSO

- Juniper Networks Vendor-Specific RADIUS Attributes | 247
- Configuring RADIUS System Accounting | 255
- Example: Configuring RADIUS Authentication | 243

Example: Configuring a RADIUS Server for System Authentication

This example shows how to configure a RADIUS server for system authentication.

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
• Configure at least one RADIUS server. For more details, see RADIUS Authentication and Accounting Servers Configuration Overview.

Overview

In this example, you add a new RADIUS server with an IP address of 172.16.98.1 and specify the shared secret password of the RADIUS server as Radiussecret1. The secret is stored as an encrypted value in the configuration database. Finally, you specify the source address to be included in the RADIUS server requests by the device. In most cases you can use the loopback address of the device, which in this example is 10.0.0.1.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system radius-server address 172.16.98.1
set system radius-server 172.16.98.1 secret Radiussecret1
set system radius-server 172.16.98.1 source-address 10.0.0.1
```

GUI Step-by-Step Procedure

To configure a RADIUS server for system authentication:

1. In the J-Web user interface, select Configure>System Properties>User Management.

2. Click Edit. The Edit User Management dialog box appears.

3. Select the Authentication Method and Order tab.

4. In the RADIUS section, click Add. The Add Radius Server dialog box appears.

5. In the IP Address box, type the server's 32-bit IP address.

6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.

7. In the Server Port box, type the appropriate port.

8. In the Source Address box, type the source IP address of the server.
9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.

10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.

11. Click OK to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click Commit Options>Commit.

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a RADIUS server for system authentication:

1. Add a new RADIUS server and set its IP address.

```
[edit system]
user@host# set radius-server address 172.16.98.1
```

2. Specify the shared secret (password) of the RADIUS server.

```
[edit system]
user@host# set radius-server 172.16.98.1 secret Radiussecret1
```

3. Specify the device's loopback address source address.

```
[edit system]
user@host# set radius-server 172.16.98.1 source-address 10.0.0.1
```

Results
From configuration mode, confirm your configuration by entering the show system radius-server command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system radius-server
radius-server 172.16.98.1 {
    secret Radiussecret1;
}
```
source-address 10.0.0.1;
}

If you are done configuring the device, enter `commit` from configuration mode.

NOTE: To completely set up RADIUS authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See “Example: Configuring Authentication Order” on page 227.
- Configure a user. See “Example: Configuring New Users” on page 95.
- Configure local user template accounts. See "Example: Creating Template Accounts" on page 213.

Verification

Confirm that the configuration is working properly.

Verifying the RADIUS Server System Authentication Configuration

Purpose
Verify that the RADIUS server has been configured for system authentication.

Action
From operational mode, enter the `show system radius-server` command.

SEE ALSO

| Junos OS User Authentication Methods | 209 |
| Junos OS User Accounts Overview | 91 |
| Configuring Local User Template Accounts for User Authentication | 210 |
| Example: Configuring a TACACS+ Server for System Authentication | 268 |
Example: Configuring RADIUS Authentication

The Junos OS supports two protocols for central authentication of users on multiple routers: RADIUS and TACACS+. We recommend RADIUS because it is a multivendor IETF standard, and its features are more widely accepted than those of TACACS+ or other proprietary systems. In addition, we recommend using a one-time-password system for increased security, and all vendors of these systems support RADIUS.

The Junos OS uses one or more template accounts to perform user authentication. You create the template account or accounts, and then configure the user access to use that account. If the RADIUS server is unavailable, the fallback is for the login process to use the local account that set up on the router or switch.

The following example shows how to configure RADIUS authentication:

```
[edit]
  system {
    authentication-order [ radius password ];
    root-authentication {
      encrypted-password "$ABC123; # SECRET-DATA
    }
    name-server {
      10.1.1.1;
      10.1.1.2;
    }
  }
```

The following example shows how to enable RADIUS authentication and define the shared secret between the client and the server. The secret enables the client and server to determine that they are talking to the trusted peer.

Define a timeout value for each server, so that if there is no response within the specified number of seconds, the router can try either the next server or the next authentication mechanism.

```
[edit]
  system {
    radius-server {
      10.1.2.1 {
        secret "$ABC123"; # SECRET-DATA
        timeout 5;
      }
      10.1.2.2 {
        secret "$ABC123"; # SECRET-DATA
        timeout 5;
      }
    }
  }
```
The following example shows how to configure RADIUS template accounts for different users or groups of users:

```plaintext
[edit]
  system {
    login {
      user observation {
        uid 1001;
        class observation;
      }
      user operation {
        uid 1002;
        class operation;
      }
      user engineering {
        uid 1003;
        class engineering;
      }
    }
  }
```

### Configuring RADIUS Authentication (QFX Series or OCX Series)

#### IN THIS SECTION

- Configuring RADIUS Server Details | 245
- Configuring MS-CHAPv2 for Password-Change Support | 246
- Specifying a Source Address for the Junos OS to Access External RADIUS Servers | 247

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. Tasks to configure RADIUS authentication are:
NOTE: The source-address statement is not supported at the [edit system radius-options] or [edit system-radius-server name] hierarchies on the QFabric system.

Configuring RADIUS Server Details

To use RADIUS authentication on the router or switch, configure information about one or more RADIUS servers on the network by including one radius-server statement at the [edit system] hierarchy level for each RADIUS server:

```
[edit system]
radius-server server-address {
  accounting-port port-number;
  port number;
  retry number;
  secret password;
  source-address source-address;
  timeout seconds;
}
```

server-address is the address of the RADIUS server.

You can specify a port on which to contact the RADIUS server. By default, port number 1812 is used (as specified in RFC 2865). You can also specify an accounting port to send accounting packets. The default is 1813 (as specified in RFC 2866).

You must specify a password in the secret password statement. If the password contains spaces, enclose it in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the amount of time that the local router or switch waits to receive a response from a RADIUS server (in the timeout statement) and the number of times that the router or switch attempts to contact a RADIUS authentication server (in the retry statement). By default, the router or switch waits 3 seconds. You can configure this to be a value from 1 through 90 seconds. By default, the router or switch retries connecting to the server three times. You can configure this to be a value from 1 through 10 times.

You can use the source-address statement to specify a logical address for individual or multiple RADIUS servers.

To configure multiple RADIUS servers, include multiple radius-server statements.
To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in “Example: Configuring Authentication Order” on page 227.

You can also configure RADIUS authentication at the [edit access] and [edit access profile] hierarchy level. Junos OS uses the following search order to determine which set of servers are used for authentication:

1. [edit access profile profile-name radius-server server-address]
2. [edit access radius-server server-address]
3. [edit system radius-server server-address]

Configuring MS-CHAPv2 for Password-Change Support

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at the next login.

Before you configure MS-CHAPv2 for password-change support, ensure that you:

- Configure the RADIUS server authentication parameters
- Set the authentication-order to use the RADIUS server for the initial password attempt

To configure MS-CHAP-v2, include the following statements at the [edit system radius-options] hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
    authentication-order [ radius password ];
    radius-server {
        192.168.69.149 secret "$ABC123"; ## SECRET-DATA
    }
    radius-options {
        password-protocol mschap-v2;
    }
    login {
        user bob {
```
Specifying a Source Address for the Junos OS to Access External RADIUS Servers

You can specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You can also specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information.

To specify a source address for a RADIUS server, include the `source-address` statement at the `[edit system radius-server server-address]` hierarchy level:

```
[edit system radius-server server-address]
source-address source-address;
```

`source-address` is a valid IP address configured on one of the router or switch interfaces.

SEE ALSO

- Juniper Networks Vendor-Specific RADIUS Attributes | 247
- Example: Configuring Authentication Order | 227
- Example: Configuring RADIUS Authentication | 243
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands | 273
- Junos OS User Authentication Methods | 209

Juniper Networks Vendor-Specific RADIUS Attributes

Junos OS supports the configuration of Juniper Networks RADIUS vendor-specific attributes (VSAs). These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 13 on page 248 lists the Juniper Networks VSAs you can configure.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper-Local-User-Name</td>
<td>Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets.</td>
<td>1</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juniper-Allow-Commands</td>
<td>Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.</td>
<td>2</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juniper-Deny-Commands</td>
<td>Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.</td>
<td>3</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>String</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Juniper-Allow-Configuration</td>
<td>Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user’s login class permission bits. This attribute is used only in Access-Accept packets.</td>
<td>4</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td>Juniper-Deny-Configuration</td>
<td>Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user’s login class permission bits. This attribute is used only in Access-Accept packets.</td>
<td>5</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td>Juniper-Interactive-Command</td>
<td>Indicates the interactive command entered by the user. This attribute is used only in Accounting-Request packets.</td>
<td>8</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td>Juniper-Configuration-Change</td>
<td>Indicates the interactive command that results in a configuration (database) change. This attribute is used only in Accounting-Request packets.</td>
<td>9</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
</tbody>
</table>
### Table 13: Juniper Networks Vendor-Specific RADIUS Attributes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper-User-Permissions</td>
<td>Contains information the server uses to specify user permissions. This attribute is used only in Access-Accept packets. NOTE: When the Juniper-User-Permissions attribute is configured to grant the Junos OS <strong>maintenance</strong> or <strong>all</strong> permissions on a RADIUS server, the UNIX wheel group membership is not automatically added to a user's list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions <strong>maintenance</strong> or <strong>all</strong>, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</td>
<td>10</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters. The string is a list of permission flags separated by a space. The exact name of each flag must be specified in its entirety. See &quot;Login Class Permission Flags&quot; on page 119.</td>
</tr>
</tbody>
</table>
Table 13: Juniper Networks Vendor-Specific RADIUS Attributes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper-Authentication-Type</td>
<td>Indicates the authentication method (local database, or RADIUS server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using RADIUS server, the attribute value shows 'remote'.</td>
<td>11</td>
<td>≥5</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td>Juniper-Session-Port</td>
<td>Indicates the source port number of the established session.</td>
<td>12</td>
<td>size of integer</td>
<td>Integer</td>
</tr>
</tbody>
</table>

For more information about the VSAs, see RFC 2138, Remote Authentication Dial In User Service (RADIUS).

Juniper-Switching-Filter VSA Match Conditions and Actions

Devices support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, Remote Authentication Dial In User Service (RADIUS).

Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are cleartext fields sent from the RADIUS server to the device as a result of authentication success or failure. Authentication prevents unauthorized user access by blocking a supplicant at the port until the device is authenticated by the RADIUS server. The VSA attributes are interpreted by the device during authentication, and the device takes appropriate actions. Implementing port-filtering attributes with authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

These port-filtering attributes specific to Juniper Networks are encapsulated in a RADIUS server VSA with the vendor ID set to the Juniper Networks ID number, 2636.

As well as configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the device directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the authentication process, and its actions are applied at the device port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and devices.
The Juniper-Switching-Filter VSA works in conjunction with 802.1X authentication to centrally control access of supplicants to the network. You can use this VSA to configure filters on the RADIUS server, which are sent to the switch and applied to users that have been authenticated using 802.1X authentication.

The Juniper-Switching-Filter VSA can contain one or more filter terms. Filter terms are configured using one or more match conditions with a resulting action. Match conditions are the criteria that a packet must meet for a configured action to be applied on it. The action is the action that the switch takes if a packet meets the criteria in the match conditions. The action that the switch can take is either accept or deny a packet.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both match and action statements are mandatory.
- If no match condition is specified, any packet is considered a match by default.
- If no action is specified, the default action is to deny the packet.
- Any or all options can be included in each match and action statement.
- The AND operation is performed on fields that are of a different type, which are separated by commas. Fields of the same type cannot be repeated.
- For the forwarding-class option to be applied, the forwarding class must be configured on the switch. If the forwarding class is not configured on the switch, this option is ignored.

Table 14 on page 252 describes the match conditions that you can specify when you configure a VSA attribute as a firewall filter by using the match command on the RADIUS server. The string that defines a match condition is called a match statement.

Table 14: Match Conditions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-mac mac-address</td>
<td>Destination media access control (MAC) address of the packet.</td>
</tr>
<tr>
<td>source-dot1q-tag tag</td>
<td>Tag value in the 802.1Q header, in the range 0 through 4095.</td>
</tr>
<tr>
<td>destination-ip ip-address</td>
<td>Address of the final destination node.</td>
</tr>
<tr>
<td>ip-protocol protocol-id</td>
<td>IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: ah, esp (8), esp (50), gre (47), icmp (1), igmp (2), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)</td>
</tr>
</tbody>
</table>
Table 14: Match Conditions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-port port</td>
<td>TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under destination-port.</td>
</tr>
<tr>
<td>destination-port port</td>
<td>TCP or UDP destination port field. Normally, you specify this match statement in conjunction with the ip-protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed): afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspsserver (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobilip-mm (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rlogin (2108), smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514), telnet (23), tacacs-ds (65), talk (517), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)</td>
</tr>
</tbody>
</table>

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 15 on page 253 shows the actions that you can specify in a term.

Table 15: Actions for VSAs

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(allow</td>
<td>deny)</td>
</tr>
<tr>
<td>forwarding-class class-of-service</td>
<td>(Optional) Classify the packet in one of the following forwarding classes:</td>
</tr>
<tr>
<td></td>
<td>• assured-forwarding</td>
</tr>
<tr>
<td></td>
<td>• best-effort</td>
</tr>
<tr>
<td></td>
<td>• expedited-forwarding</td>
</tr>
<tr>
<td></td>
<td>• network-control</td>
</tr>
</tbody>
</table>
Table 15: Actions for VSAs (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loss-priority (low</td>
<td>medium</td>
</tr>
</tbody>
</table>

SEE ALSO

- Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395
- Understanding Dynamic Filters Based on RADIUS Attributes | 405

Understanding RADIUS Accounting

Devices support IETF RFC 2866, RADIUS Accounting. Configuring RADIUS accounting on the device supports collecting statistical data about users logging in to or out from a LAN and sending the data to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, analyzing and tracking usage patterns, or billing a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the device, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Junos OS.

The RADIUS accounting process between the device and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. The device forwards an accounting-request packet containing an event record to the accounting server. The event record associated with this supplicant contains an Acct-Status-Type attribute whose value indicates the beginning of user service for this supplicant. When the supplicant's session ends, the accounting request contains an Acct-Status-Type attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.
3. The RADIUS accounting server logs these events in a file as start-accounting or stop-accounting records. On FreeRADIUS, the filename is the server's address; for example, 192.0.2.0.

4. The accounting server sends an accounting-response packet back to the device confirming it has received the accounting request.

5. If the device does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

SEE ALSO

   Configuring RADIUS System Accounting | 255

Configuring RADIUS System Accounting

With RADIUS accounting enabled, Juniper Networks routers or switches, acting as RADIUS clients, can notify the RADIUS server about user activities such as software logins, configuration changes, and interactive commands. The framework for RADIUS accounting is described in RFC 2866.

Tasks for configuring RADIUS system accounting are:

1. Configuring Auditing of User Events on a RADIUS Server | 255
2. Specifying RADIUS Server Accounting and Auditing Events | 256
3. Configuring RADIUS Server Accounting | 256

Configuring Auditing of User Events on a RADIUS Server

To audit user events, include the following statements at the [edit system accounting] hierarchy level:

```bash
[edit system accounting]
events { [ events ];
    destination {
        radius {
            server {
                server-address {
```
Specifying RADIUS Server Accounting and Auditing Events

To specify the events you want to audit when using a RADIUS server for authentication, include the `events` statement at the `[edit system accounting]` hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring RADIUS Server Accounting

To configure RADIUS server accounting, include the `server` statement at the `[edit system accounting destination radius]` hierarchy level:

```
server [ server-address { accounting-port port-number; retry number; routing-instance routing-instance; secret password; source-address address; timeout seconds; } ]
```
server-address specifies the address of the RADIUS server. To configure multiple RADIUS servers, include multiple server statements.

NOTE: If no RADIUS servers are configured at the [edit system accounting destination radius] statement hierarchy level, the Junos OS uses the RADIUS servers configured at the [edit system radius-server] hierarchy level.

accounting-port port-number specifies the RADIUS server accounting port number.

The default port number is 1813.

NOTE: If you enable RADIUS accounting at the [edit access profile profile-name accounting-order] hierarchy level, accounting is triggered on the default port of 1813 even if you do not specify a value for the accounting-port statement.

routing-instance routing-instance is the name of the non-default management instance. Use mgmt_junos as the routing-instance name. See Management Interface in a Nondefault Instance.

You must specify a secret (password) that the local router or switch passes to the RADIUS client by including the secret statement. If the password contains spaces, enclose the entire password in quotation marks (" ").

In the source-address statement, specify a source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address (in case if radius-server address is IPv4) or IPv6 address (in case if radius-server address is IPv6) configured on one of the router or switch interfaces.

Optionally, you can specify the number of times that the router or switch attempts to contact a RADIUS authentication server by including the retry statement. By default, the router or switch retries three times. You can configure the router or switch to retry from 1 through 10 times.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a RADIUS server by including the timeout statement. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

Starting with Junos OS Release 14.1 and Junos OS Release 17.3R1, you can configure the enhanced-accounting statement to view the attribute values of a logged in user. If you use the enhanced-accounting statement at the [edit system radius-options] hierarchy level, the RADIUS attributes such as access method, remote port, and access privileges can be audited. You can limit the number of attribute values to be displayed for auditing by using the enhanced-avs-max <number> statement at the [edit system accounting] hierarchy level.
When a Juniper Networks router or switch is configured with RADIUS accounting, it sends **Accounting-Start** and **Accounting-Stop** messages to the RADIUS server. These messages contain information about user activities such as software logins, configuration changes, and interactive commands. This information is typically used for monitoring a network, collecting usage statistics, and ensuring that users are billed properly.

The following example shows three servers (10.5.5.5, 10.6.6.6, and 10.7.7.7) configured for RADIUS accounting:

```plaintext
system {
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      radius {
        server {
          10.5.5.5 {
            accounting-port 3333;
            secret $ABC123;
            source-address 10.1.1.1;
            retry 3;
            timeout 3;
          }
          10.6.6.6 secret $ABC123;
          10.7.7.7 secret $ABC123;
        }
      }
    }
  }
}
```
### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 18.1R1, existing RADIUS behavior is enhanced to support a management interface in a non-default VRF instance.</td>
</tr>
<tr>
<td>14.1</td>
<td>Starting with Junos OS Release 14.1 and Junos OS Release 17.3R1, you can configure the enhanced-accounting statement to view the attribute values of a logged in user.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- Junos OS User Authentication Overview | 209
- Authentication Order for RADIUS, TACACS+, and Local Password | 218
- TACACS+ Authentication | 263

### RADIUS over TLS (RADSEC)

**IN THIS SECTION**
- Configure the RADSEC Destination | 260
- Configure TLS Connection Parameters | 261
- Example: Simple RADSEC Configuration | 262
- Monitoring Certificates | 262
- Monitoring RADSEC Destinations | 263

RADIUS over TLS is designed to provide secure communication of RADIUS requests using the Transport Secure Layer (TLS) protocol. RADIUS over TLS, also known as RADSEC, redirects regular RADIUS traffic to remote RADIUS servers connected over TLS. RADSec allows RADIUS authentication, authorization and accounting data to be passed safely across untrusted networks.

RADSEC uses TLS in combination with the Transmission Control Protocol (TCP). This transport profile provides stronger security than the User Datagram Protocol (UDP) which was originally used for RADIUS transmission. RADIUS over UDP encrypts the shared secret password using the MD5 algorithm, which is
vulnerable to attacks. RADSEC mitigates the risk of attacks on MD5 by exchanging RADIUS packet payloads over an encrypted TLS tunnel.

**NOTE:** Due to limitations of the TCP protocol, RADSEC can have no more than 255 RADIUS messages in flight.

### Configure the RADSEC Destination

RADSEC servers are represented by RADSEC destination objects. To configure RADSEC, you must define the RADSEC server as a destination, and direct RADIUS traffic to that destination.

You define the RADSEC server as a destination using the `radsec` statement at the `[edit access]` hierarchy level. RADSEC destinations are identified by a unique numeric ID. You can configure multiple RADSEC destinations with different parameters pointing to the same RADSEC server.

To redirect traffic from a standard RADIUS server to a RADSEC server, associate the RADIUS server with a RADSEC destination. For example, the RADIUS server `1.1.1.1` is associated with RADSEC destination `10`:

```plaintext
access {
  radius-server 1.1.1.1 {
    secret zzz;
    radsec-destination 10;
  }
}
```

You can also associate the RADIUS server with a RADSEC destination inside an access profile. For example, RADIUS server `2.2.2.2` in profile `acc_profile` is associated with RADSEC destination `10`:

```plaintext
access {
  profile acc_profile {
    secret zzz;
    radsec-destination 10;
  }
}
```

**NOTE:** You can redirect more than one RADIUS server to the same RADSEC destination.
To configure RADSEC:

1. Configure the RADSEC destination with a unique ID and an IP address.

   [edit access]
   user@host# radsec destination id-number address server-address

2. Configure the port of the RADSEC server. If no port is configured, the default RADSEC port 2083 is used.

   [edit access radsec destination id-number]
   user@host# port port-number

3. Redirect traffic from a RADIUS server to the RADSEC destination:

   [edit access]
   user@host# radius-server server-address radsec-destination id-number

---

Configure TLS Connection Parameters

The TLS connection provides encryption, authentication, and data integrity for the exchange of RADIUS messages. TLS relies on certificates and private-public key exchange pairs to secure the transmission of data between the RADSEC client and server. The RADSEC destination uses local certificates that are dynamically acquired from the Junos PKI infrastructure.

To enable RADSEC, you must specify the name of the local certificate. For information on configuring the local certificate and certificate authority (CA), see Configuring Digital Certificates.

1. Specify the name of the local certificate to be used for TLS communications.

   [edit access]
   user@host# radsec destination id-number tls-certificate certificate-name

2. Configure the certified name of the RADSEC server.

   [edit access]
   user@host# radsec destination id-number tls-peer-name cert-server-name
3. (Optional) Configure the TLS connection timeout (default is 5 seconds).

```
[edit access]
user@host# radsec destination id-number tls-timeout seconds
```

### Example: Simple RADSEC Configuration

The following example is a simple RADSEC configuration with one RADIUS server and one RADSEC destination. RADIUS traffic is redirected from RADIUS server 1.1.1.1 to RADSEC destination 10.

```
access {
    radius-server 1.1.1.1 {
        secret zzz;
        radsec-destination 10;
    }
    radsec {
        destination 10 {
            address 10.1.1.1;
            max-tx-buffers 1000;
            id-reuse-timeout 30;
            port 1777;
            source-address 1.1.1.2;
            tls-certificate my_cert;
            tls-force-ciphers { medium | low };
            tls-min-version { v1.1 | v1.2 };
            tls-peer-name x0.radsec.com
            tls-timeout 10;
        }
    }
}
```

### Monitoring Certificates

To view information about the state and statistics of local certificate acquisition: `show network-access radsec local-certificate`. 
Monitoring RADSEC Destinations

To view statistics for the RADSEC destinations: `show network-access radsec statistics`.

To view the state of the RADSEC destinations: `show network-access radsec state`.

RELATED DOCUMENTATION

- Example: Configuring RADIUS Authentication | 243
- Example: Configuring System Authentication for RADIUS, TACACS+, and Password Authentication | 230
- Example: Configuring Authentication Order | 227
- Example: Configuring RADIUS Authentication | 243

TACACS+ Authentication

IN THIS SECTION

- Configuring TACACS+ Authentication | 264
- Example: Configuring a TACACS+ Server for System Authentication | 268
- Configuring Periodic Refresh of the TACACS+ Authorization Profile | 271
- Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands | 273
- Juniper Networks Vendor-Specific TACACS+ Attributes | 276
- Configuring TACACS+ System Accounting | 278

The Junos OS supports TACACS+ for central authentication of users on multiple routers or switches or security devices. To use TACACS+ authentication on the device, you must configure information about one or more TACACS+ servers on the network. You can also configure TACACS+ accounting on the device to collect statistical data about the users logging in to or out from a LAN and sending the data to a TACACS+ accounting server. For more information, read this topic.
Configuring TACACS+ Authentication

TACACS+ authentication is a method of authenticating users who attempt to access the router or switch.

NOTE: Starting with Release 13.3, Junos OS supports IPv6 along with the existing IPv4 support for user authentication using TACACS+ servers.

Tasks to configure TACACS+ configuration are:

Configuring TACACS+ Server Details

To use TACACS+ authentication on the router or switch, configure information about one or more TACACS+ servers on the network by including the tacplus-server statement at the [edit system] hierarchy level:

```
[edit system]
tacplus-server server-address {
    port port-number;
    routing-instance routing-instance;
    secret password;
    single-connection;
    timeout seconds;
}
```

*server-address* is the address of the TACACS+ server.

*port-number* is the TACACS+ server port number.

*routing-instance routing-instance* is the name of the routing instance used to send and receive TACACS+ packets. By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+
through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos. For more information on this VRF management instance, see “Configuring TACACS+ to Use the Management Instance” on page 266. Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in authentication.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the secret statement. If the password included spaces, enclose the password in quotation marks. The secret used by the local router or switch must match that used by the server.

Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the timeout statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can have the software maintain one open Transmission Control Protocol (TCP) connection to the server for multiple requests, rather than opening a connection for each connection attempt by including the single-connection statement.

NOTE: Early versions of the TACACS+ server do not support the single-connection option. If you specify this option and the server does not support it, the Junos OS will be unable to communicate with that TACACS+ server.

To configure multiple TACACS+ servers, include multiple tacplus-server statements.

On a TX Matrix router, TACACS+ accounting should be configured only under the groups re0 and re1.

NOTE: Accounting should not be configured at the [edit system] hierarchy level; on a TX Matrix router, control is done under the switch-card chassis only.

To configure a set of users that share a single account for authorization purposes, you create a template user. To do this, include the user statement at the [edit system login] hierarchy level, as described in “Example: Configuring Authentication Order” on page 227.

SEE ALSO

routing-instance (Accounting and Authentication)
Configuring TACACS+ to Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.

```
[edit system]
tacplus-server server-address {
    routing-instance routing-instance;
}
```

When the `routing-instance mgmt_junos` option is configured in both the `tacplus-server server-address` and the `tacplus server server-ip` statements (see `tacplus`), provided the `management-instance` statement is also configured, TACACS+ packets are routed through the management instance mgmt_junos.

**NOTE:** The `routing-instance mgmt_junos` option must be configured in both the `tacplus-server` and the `tacplus server` statements. If not, even when the `management-instance` statement is configured, TACACS+ packets use the default routing instance only.

Before Junos OS Release 17.4R1, there is no option for configuring a routing instance for TACACS+. Therefore, even if `management-instance` is configured, there is no TACACS+ routing instance functionality, until Junos OS Release 17.4R1.

For more details on the management instance mgmt_junos, see `management-instance`.

Specifying a Source Address for the Junos OS to Access External TACACS+ Servers

You can specify which source address the Junos OS uses when accessing your network to contact an external TACACS+ server for authentication. You can also specify which source address the Junos OS uses when contacting a TACACS+ server for sending accounting information.

To specify a source address for a TACACS+ server for authentication, include the `source-address` statement at the `[edit system tacplus-server server-address]` hierarchy level:

```
[edit system tacplus-server server-address]
source-address source-address;
```

`source-address` is a valid IP address configured on one of the router or switch interfaces.

To specify a source address for a TACACS+ server for system accounting, include the `source-address` statement at the `[edit system accounting destination tacplus server server-address]` hierarchy level:
source-address is a valid IP address configured on one of the router or switch interfaces.

Configuring the Same Authentication Service for Multiple TACACS+ Servers

To configure the same authentication service for multiple TACACS+ servers, include statements at the [edit system tacplus-server] and [edit system tacplus-options] hierarchy levels. For information about how to configure a TACACS+ server at the [edit system tacplus-server] hierarchy level, see “Configuring TACACS+ Authentication” on page 264.

To assign the same authentication service to multiple TACACS+ servers, include the service-name statement at the [edit system tacplus-options] hierarchy level:

```
[edit system tacplus-options]
    service-name service-name;
```

service-name is the name of the authentication service. By default, the service name is set to junos-exec.

The following example shows how to configure the same authentication service for multiple TACACS+ servers:

```
[edit system]
    tacplus-server {
        10.2.2.2 secret "$ABC123"; ## SECRET-DATA
        10.3.3.3 secret "$ABC123";## SECRET-DATA
    }
    tacplus-options {
        service-name bob;
    }
```

Configuring Juniper Networks Vendor-Specific TACACS+ Attributes

The Juniper Networks Vendor-Specific TACACS+ Attributes enable you to configure access privileges for users on a TACACS+ server. They are specified in the TACACS+ server configuration file on a per-user basis. The Junos OS retrieves these attributes through an authorization request of the TACACS+ server after authenticating a user. You do not need to configure these attributes to run the Junos OS with TACACS+.

To specify these attributes, include a service statement of the following form in the TACACS+ server configuration file:
This service statement can appear in a user or group statement.

Example: Configuring a TACACS+ Server for System Authentication

IN THIS SECTION
- Requirements | 268
- Overview | 268
- Configuration | 269
- Verification | 271

This example shows how to configure a TACACS+ server for system authentication.

Requirements

Before you begin:

- Perform the initial device configuration. See the Getting Started Guide for your device.
- Configure at least one TACACS+ server.

Overview

In this example, you set the IP address to 172.16.98.24 and the shared secret password of the TACACS+ server to Tacacssecret1. The secret password is stored as an encrypted value in the configuration database. You then set the loopback source address as 10.0.0.1
Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system tacplus-server address 172.16.98.24
set system tacplus-server 172.16.98.24 secret Tacacsssecret1
set system tacplus-server 172.16.98.24 source-address 10.0.0.1
```

GUI Step-by-Step Procedure
To configure a TACACS+ server for system authentication:

1. In the J-Web user interface, select **Configure>System Properties>User Management**.

2. Click **Edit**. The Edit User Management dialog box appears.

3. Select the **Authentication Method and Order** tab.

4. In the TACACS section, click **Add**. The Add TACACS Server dialog box appears.

5. In the IP Address box, type the server’s 32-bit IP address.

6. In the Password and Confirm Password boxes, type the secret password for the server and verify your entry.

7. In the Server Port box, type the appropriate port.

8. In the Source Address box, type the locally configured interface address, which is used as the source address for TACACS+ packets.

   **NOTE:** The Source Address box can accept either a hostname or an IP address.

9. In the Retry Attempts box, specify the number of times that the server should try to verify the user's credentials.

10. In the Time Out box, specify the amount of time (in seconds) the device should wait for a response from the server.
11. Click **OK** to check your configuration and save it as a candidate configuration.

12. If you are done configuring the device, click **Commit Options>Commit**.

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a TACACS+ server for system authentication:

1. Add a new TACACS+ server and set its IP address.

```
[edit system]
user@host# set tacplus-server address 172.16.98.24
```

2. Specify the shared secret (password) of the TACACS+ server.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 secret Tacacssecret1
```

3. Specify the device’s loopback address as the source address.

```
[edit system]
user@host# set tacplus-server 172.16.98.24 source-address 10.0.0.1
```

**Results**

From configuration mode, confirm your configuration by entering the `show system tacplus-server` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system tacplus-server
tacplus-server 172.16.98.24 {  
  secret Tacacssecret1;  
  source-address 10.0.0.1;  
}
```

If you are done configuring the device, enter **commit** from configuration mode.
NOTE: To completely set up TACACS+ authentication, you must create user template accounts and specify a system authentication order. Do one of the following tasks:

- Configure a system authentication order. See "Example: Configuring Authentication Order" on page 227.
- Configure a user. See "Example: Configuring New Users" on page 95.
- Configure local user template accounts. See "Example: Creating Template Accounts" on page 213.

Verification

Confirm that the configuration is working properly.

**Verifying the TACACS+ Server System Authentication Configuration**

**Purpose**

Verify that the TACACS+ server has been configured for system authentication.

**Action**

From configuration mode, enter the `show system tacplus-server` command.

SEE ALSO

- Junos OS User Authentication Methods | 209
- Junos OS User Accounts Overview | 91
- Configuring Local User Template Accounts for User Authentication | 210

**Configuring Periodic Refresh of the TACACS+ Authorization Profile**

When you configure a Junos device to use a TACACS+ server for authentication, the device prompts users for login information, which is verified by the TACACS+ server. After the user is successfully authenticated, the JUNOS device sends an authorization request to the TACACS+ server to obtain the authorization profile for the user. Authorization profiles specify the access permissions for authenticated users or devices.

The TACACS+ server sends the authorization profile as part of an authorization response message. The remote user configured on the TACACS+ server is mapped to a local user configured on the JUNOS device.
The JUNOS device combines the remote authorization profile with the locally-configured authorization profile for the user, which is configured at the [edit system login class] hierarchy level.

The exchange of authorization request and response messages occurs only once, after successful authentication, by default. You can configure the JUNOS device to periodically fetch the remote authorization profile from the TACACS+ server and refresh the authorization profile stored locally. This ensures that any change in the authorization parameters are reflected on the local device without the user having to restart the authentication process.

To enable periodic refresh of the authorization profile, you must set the time interval at which the JUNOS device checks the authorization profile configured remotely on the TACACS+ server. If there is a change in the remote authorization profile, the device fetches the authorization profile from the TACACS+ server and the authorization profile configured under the login class hierarchy. The device refreshes the authorization profile stored locally by combining the remote and locally-configured authorization profiles.

The time interval can be configured directly on the TACACS+ server or locally on the JUNOS device using the CLI. The time interval is configured in minutes, in the range of 15 to 1440 minutes.

- To configure periodic refresh of the authorization profile on the local device using the CLI, include the `authorization-time-interval` statement at the [edit system tacplus-options] hierarchy level:

```plaintext
[edit system tacplus-options]
authorization-time-interval [minutes];
```

- To configure the time interval for periodic refresh on the TACACS+ server, add the time interval as a parameter in the authorization profile using the following syntax:

```plaintext
refresh-time-interval=minutes
```
Use the following guidelines to determine which time interval configuration takes precedence:

- If there is no refresh time interval configured on the TACACS server for periodic refresh, the JUNOS device does not receive the time interval value in the authorization response. In this case, the value configured locally on the JUNOS device will take effect.
- If the refresh time interval is configured on the TACACS server and there is no refresh time interval configured locally on the JUNOS device, the value configured on the TACACS server will take effect.
- If refresh time interval is configured on the TACACS server and also on the JUNOS device locally, the value configured on the TACACS server will take precedence.
- If there is no refresh time interval configured on the TACACS server and there is no refresh time interval configured on the JUNOS device, there will be no periodic refresh.
- If the refresh time interval configured on the TACACS server is out of range or invalid, the refresh time interval value configured locally will take effect.
- If the refresh time interval configured on the TACACS server is out of range or invalid and there is no refresh time interval configured locally, there will be no periodic refresh.

After the periodic refresh time interval is set, if the user changes the refresh interval before the authorization request is sent from the JUNOS device, the updated refresh interval takes effect after the next immediate periodic refresh.

SEE ALSO

- Defining Junos OS Login Classes | 73
- authorization-time-interval | 1530

Using Regular Expressions on a RADIUS or TACACS+ Server to Allow or Deny Access to Commands

Use regular expressions to specify which operational or configuration mode commands are allowed or denied when you use a RADIUS or TACACS+ server for user authentication. You can specify the regular expressions using the appropriate Juniper Networks vendor-specific RADIUS or TACACS+ attributes in your authentication server configuration.

The following attributes are supported for configuring authorizations on RADIUS and TACACS+ servers:

- user-permissions
- allow-configuration
• deny-configuration
• allow-commands
• deny-commands
• allow-configuration-regexp
• deny-configuration-regexp
• (TACACS+ only) allow-commands-regexp
• (TACACS+ only) deny-commands-regexp

You can specify allow-configuration, deny-configuration, allow-commands, or deny-commands in a single extended regular expression, enclosing multiple commands in parentheses and separating them using the pipe symbol. For example, you can specify multiple allow-commands parameters using: allow-commands= (cmd1 | cmd2 | cmdn). You can specify user-permissions as a list of comma-separated values, and not as a regular expression.

To configure authorizations using the allow/deny-configuration-regexps or allow/deny-commands-regexps attributes, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. For example, you can specify multiple parameters for allow-commands-regexp using the following syntax: allow-commands-regexps = ("regexp1" "regexp2" ...).

On a RADIUS or TACACS+ server, you can also use a simplified version for regular expressions where you specify each individual expression on a separate line. The simplified version is valid for allow-commands, deny-commands, allow-configuration, deny-configuration, and permissions vendor-specific attributes.

For a RADIUS server, specify the individual regular expressions using the following syntax:

For TACACS+ server, specify the individual regular expressions using the following syntax:
allow-commands1="cmd1"
allow-commands2="cmd2"
allow-commandsn="cmdn"
dery-commands1="cmd1"
dery-commands2="cmd2"
dery-commandsn="cmdn"
allow-configuration1="regex1"
allow-configuration2="regex2"
allow-configurationn="rege

dery-configuration1="regex1"
dery-configuration2="regex2"
dery-configurationn="regexn"
user-permissions1="permission-flag1"
user-permissions2="permission-flag2"
user-permissionsn="permission-flags"

NOTE:
• Numeric values 1 to n in the syntax (for TACACS+ server) must be unique but need not be sequential. For example, the following syntax is valid:

  allow-commands1="cmd1"
  allow-commands3="cmd3"
  allow-commands2="cmd2"
dery-commands3="cmd3"
dery-commands2="cmd2"
dery-commands1="cmd1"

• The limit on the number of lines of individual regular expressions is imposed by the TACACS+ or RADIUS server.

• When you issue the show cli authorization command, the command output displays the regular expression in a single line, even if you specify each individual expression on a separate line.

For more information about Juniper Networks vendor-specific RADIUS and TACACS+ attributes, see "Juniper Networks Vendor-Specific RADIUS Attributes" on page 247 and "Juniper Networks Vendor-Specific TACACS+ Attributes" on page 276.
NOTE: When RADIUS or TACACS+ authentication is configured for a router, regular expressions configured on the RADIUS or TACACS+ server merge with any regular expressions configured on the local router at the [edit system login class] hierarchy level using the allow-commands, deny-commands, allow-configuration, deny-configuration, or permissions statements. If the final expression has a syntax error, the overall result is an invalid regular expression.

SEE ALSO

Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication | 218

Juniper Networks Vendor-Specific TACACS+ Attributes

Junos OS supports the configuration of Juniper Networks TACACS+ vendor-specific attributes (VSAs). These VSAs are encapsulated in a TACACS+ vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. Table 16 on page 276 lists the Juniper Networks VSAs you can configure.

Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-user-name</td>
<td>Indicates the name of the user template used by this user when logging in to a device.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td>allow-commands</td>
<td>Contains an extended regular expression that enables the user to run operational mode commands in addition to those commands authorized by the user’s login class permission bits.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
</tbody>
</table>
### Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-configuration</td>
<td>Contains an extended regular expression that enables the user to run configuration mode commands in addition to those commands authorized by the user’s login class permission bits.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td>deny-commands</td>
<td>Contains an extended regular expression that denies the user permission to run operational mode commands authorized by the user’s login class permission bits.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
<tr>
<td>deny-configuration</td>
<td>Contains an extended regular expression that denies the user permission to run configuration mode commands authorized by the user’s login class permission bits.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters, in the form of an extended regular expression. See “Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies” on page 128.</td>
</tr>
</tbody>
</table>
Table 16: Juniper Networks Vendor-Specific TACACS+ Attributes (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Length</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-permissions</td>
<td>Contains information the server uses to specify user permissions.</td>
<td>≥3</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td></td>
<td>NOTE: When the user-permissions attribute is configured to grant the Junos OS maintenance or all permissions on an IPv4 or IPv6 TACACS+ server, the UNIX wheel group membership is not automatically added to a user’s list of group memberships. Some operations such as running the su root command from a local shell require wheel group membership permissions. However, when a user is configured locally with the permissions maintenance or all, the user is automatically granted membership to the UNIX wheel group. Therefore, we recommend that you create a template user account with the required permissions and associate individual user accounts with the template user account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication-type</td>
<td>Indicates the authentication method (local database, or TACACS+ server) used to authenticate a user. If the user is authenticated using a local database, the attribute value shows 'local'. If the user is authenticated using TACACS+ server, the attribute value shows 'remote'.</td>
<td>≥5</td>
<td>One or more octets containing printable ASCII characters.</td>
</tr>
<tr>
<td>session-port</td>
<td>Indicates the source port number of the established session.</td>
<td>size of integer</td>
<td>Integer</td>
</tr>
</tbody>
</table>

Configuring TACACS+ System Accounting

You can use TACACS+ to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
destination {
    tacplus {
```
server {
    server-address {
        port port-number;  // port number
        routing-instance routing-instance;  // routing instance
        secret password;  // secret
        single-connection;  // single connection
        timeout seconds;  // timeout
    }
}
}

Tasks for configuring TACACS+ system accounting are:

1. Specifying TACACS+ Auditing and Accounting Events | 279
2. Configuring TACACS+ Server Accounting | 279
3. Configuring TACACS+ To Use the Management Instance | 281
4. Configuring TACACS+ Accounting on a TX Matrix Router | 282

Specifying TACACS+ Auditing and Accounting Events

To specify the events you want to audit when using a TACACS+ server for authentication, include the `events` statement at the [edit system accounting] hierarchy level:

```
[edit system accounting]
events [ events ];
```

events is one or more of the following:

- **login**—Audit logins
- **change-log**—Audit configuration changes
- **interactive-commands**—Audit interactive commands (any command-line input)

Configuring TACACS+ Server Accounting

To configure TACACS+ server accounting, include the `server` statement at the [edit system accounting destination tacplus] hierarchy level:

```
[edit system accounting destination tacplus]
server {
```
server-address specifies the address of the TACACS+ server. To configure multiple TACACS+ servers, include multiple server statements.

NOTE: If no TACACS+ servers are configured at the [edit system accounting destination tacplus] statement hierarchy level, the Junos OS uses the TACACS+ servers configured at the [edit system tacplus-server] hierarchy level.

We recommend that you add the following configuration at the [edit system accounting destination tacplus] statement hierarchy level to identify a destination and help avoid generating an error condition:

```conf
accounting {
    events [ login change-log interactive-commands ];
    destination {
        tacplus;
    }
}
```

port-number specifies the TACACS+ server port number.

routing-instance routing-instance is the name of the routing instance used to send and receive TACACS+ packets. By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos. For more information on this VRF management instance, see “Configuring TACACS+ To Use the Management Instance” on page 281. Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in accounting.

You must specify a secret (password) that the local router or switch passes to the TACACS+ client by including the secret statement. If the password contains spaces, enclose the entire password in quotation marks (" "). The password used by the local router or switch must match that used by the server.
Optionally, you can specify the length of time that the local router or switch waits to receive a response from a TACACS+ server by including the `timeout` statement. By default, the router or switch waits 3 seconds. You can configure this to be a value in the range from 1 through 90 seconds.

Optionally, you can maintain one open TCP connection to the server for multiple requests, rather than opening a connection for each connection attempt, by including the `single-connection` statement.

To ensure that start and stop requests for accounting of login events are correctly logged in the Accounting file instead of the Administration log file on a TACACS+ server, include either the `no-cmd-attribute-value` statement or the `exclude-cmd-attribute` at the `[edit system tacplus-options]` hierarchy level.

If you use the `no-cmd-attribute-value` statement, the value of the `cmd` attribute is set to a null string in the start and stop requests. If you use the `exclude-cmd-attribute` statement, the `cmd` attribute is totally excluded from the start and stop requests. Both statements support the correct logging of accounting requests in the Accounting file, instead of the Administration file.

```plaintext
[edit system tacplus-options]
(no-cmd-attribute-value | exclude-cmd-attribute);
```

### Configuring TACACS+ To Use the Management Instance

By default, Junos OS routes authentication, authorization, and accounting packets for TACACS+ through the default routing instance. Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.

```plaintext
[edit system accounting destination tacplus]
server {
  server-address {
    routing-instance routing-instance;
  }
}
```

When the `routing-instance mgmt_junos` option is configured in both the `tacplus-server server-address` and the `tacplus server server-ip` statements, provided the `management-instance` statement is also configured, TACACS+ packets are routed through the management instance mgmt_junos.

**NOTE:** The `routing-instance mgmt_junos` option must be configured in both the `tacplus-server` and the `tacplus server` statements. If not, even if the `management-instance` statement is set, TACACS+ packets will still be sent using the default routing instance only.

For more details on this management instance, see `management-instance`. 
Configuring TACACS+ Accounting on a TX Matrix Router

On a TX Matrix router, TACACS+ accounting should be configured only under the groups re0 and re1.

NOTE: Accounting should not be configured at the [edit system] hierarchy; on a TX Matrix router, control is done under the switch-card chassis only.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.2R1</td>
<td>Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in authentication.</td>
</tr>
<tr>
<td>18.2R1</td>
<td>Starting in Junos OS Release 18.2R1, you can route TACACS+ traffic through any routing instance you configure in accounting.</td>
</tr>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos.</td>
</tr>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.</td>
</tr>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support routing TACACS+ packets through a management interface in a non-default VRF instance named mgmt_junos.</td>
</tr>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 17.4R1, existing TACACS+ behavior is enhanced to support a management interface in a non-default VRF instance.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- Junos OS User Authentication Overview | 209
- Authentication Order for RADIUS, TACACS+, and Local Password | 218
- RADIUS Authentication | 233
Authentication for Routing Protocols

You can configure an authentication method and password for routing protocol messages for IGPs, IS-IS, OSPF, and RIP, and RSVP. To prevent exchange of unauthenticated or forged packets, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. Read this topic for more information.

Junos OS Authentication Methods for Routing Protocols

Some interior gateway protocols (IGPs)—Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)—and Resource Reservation Protocol (RSVP) allow you to configure an authentication method and password. Neighboring routers use the password to verify the authenticity of packets sent by the protocol from the router or from a router interface. The following authentication methods are supported:

- **Simple authentication (IS-IS, OSPF, and RIP)**—Uses a simple text password. The receiving router uses an authentication key (password) to verify the packet. Because the password is included in the transmitted packet, this method of authentication is relatively insecure. We recommend that you not use this authentication method.

- **MD5 and HMAC-MD5 (IS-IS, OSPF, RIP, and RSVP)**—Message Digest 5 (MD5) creates an encoded checksum that is included in the transmitted packet. HMAC-MD5, which combines HMAC authentication with MD5, adds the use of an iterated cryptographic hash function. With both types of authentication, the receiving router uses an authentication key (password) to verify the packet. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

In general, authentication passwords are text strings consisting of a maximum of 16 or 255 letters and digits. Characters can include any ASCII strings. If you include spaces in a password, enclose all characters in quotation marks (" ").
Junos-FIPS has special password requirements. FIPS passwords must be between 10 and 20 characters in length. Passwords must use at least three of the five defined character sets (uppercase letters, lowercase letters, digits, punctuation marks, and other special characters). If Junos-FIPS is installed on the router, you cannot configure passwords unless they meet this standard.

Example: Configuring the Authentication Key for BGP and IS-IS Routing Protocols

The main task of a router is to use its routing and forwarding tables to forward user traffic to its intended destination. Attackers can send forged routing protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn can degrade the functionality of the router and the network. To prevent such attacks, routers must ensure that they form routing protocol relationships (peering or neighboring relationships) to trusted peers. One way of doing this is by authenticating routing protocol messages. We strongly recommend using authentication when configuring routing protocols. The Junos OS supports HMAC-MD5 authentication for BGP, Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Resource Reservation Protocol (RSVP). HMAC-MD5 uses a secret key that is combined with the data being transmitted to compute a hash. The computed hash is transmitted along with the data. The receiver uses the matching key to recompute and validate the message hash. If an attacker has forged or modified the message, the hash will not match and the data will be discarded.

In the following examples, we configure BGP as the exterior gateway protocol (EGP) and IS-IS as the interior gateway protocol (IGP). If you use OSPF, configure it similarly to the IS-IS configuration shown.

Configuring BGP

The following example shows the configuration of a single authentication key for the BGP peer group internal peers. You can also configure BGP authentication at the neighbor or routing instance levels, or for all BGP sessions. As with any security configuration, there is a trade-off between the degree of granularity (and to some extent the degree of security) and the amount of management necessary to maintain the system. This example also configures a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.

```bash
[edit]
protocols {
    bgp {
        group ibgp {
            type internal;
        }
    }
}
```
Configuring IS-IS

Although all IGPs supported by the Junos OS support authentication, some are inherently more secure than others. Most service providers use OSPF or IS-IS to allow fast internal convergence and scalability and to use traffic engineering capabilities with Multiprotocol Label Switching (MPLS). Because IS-IS does not operate at the network layer, it is more difficult to spoof than OSPF, which is encapsulated in IP and is therefore subject to remote spoofing and DoS attacks.

The following example also shows how to configure a number of tracing options for routing protocol events and errors, which can be good indicators of attacks against routing protocols. These events include protocol authentication failures, which might point to an attacker that is sending spoofed or otherwise malformed routing packets to the router in an attempt to elicit a particular behavior.
Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols

You can configure an authentication key update mechanism for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. This mechanism allows you to update authentication keys without interrupting associated routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

To configure this feature, include the `authentication-key-chains` statement at the [edit security] level, and include the `authentication-algorithm algorithm` and `authentication-key-chain` statements for the BGP or LDP routing protocols at the [edit protocols] level.

The following topics provide more details about configuring authentication key updates for BGP and LDP Routing Protocols:

- Configuring Authentication Key Updates on page 287
Configuring Authentication Key Updates

To configure the authentication key update mechanism, include the **key-chain** statement at the [edit security authentication-key-chains] hierarchy level, and specify the **key** option to create a keychain consisting of several authentication keys.

```
[edit security authentication-key-chains]
key-chain key-chain-name {
    key key {
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
    }
}
```

**key-chain**—Assigns a name to the keychain mechanism. This name is also configured at the [edit protocols bgp] or the [edit protocols ldp] hierarchy levels to associate unique authentication **key-chain** attributes as specified using the following options:

- **key**—Each key within a keychain is identified by a unique integer value. The range is from 0 through 63.
- **secret**—Each key must specify a secret in encrypted text or plain text format. Even if you enter the secret data in plain-text format, the secret always appears in encrypted format.
- **start-time**—Start times for authentication key updates are specified in UTC (Coordinated Universal Time), and must be unique within the keychain.

Configuring BGP and LDP for Authentication Key Updates

To configure the authentication key update mechanism for the BGP and LDP routing protocols, include the **authentication-key-chain** statement at the [edit protocols (bgp | ldp)] hierarchy level to associate each routing protocol with the [edit security authentication-key-chains] authentication keys. You must also configure the **authentication-algorithm algorithm** statement at the [edit protocols (bgp | ldp)] hierarchy level.

```
[edit protocols (bgp | ldp)]
group group-name {
    neighbor address {
        authentication-algorithm algorithm;
        authentication-key-chain key-chain-name;
    }
}
```
NOTE: When configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

For information about the BGP protocol, see the Junos OS Routing Protocols Library.

RELATED DOCUMENTATION

- authentication-algorithm
- authentication-key-chain (Protocols BGP and BMP)
- authentication-key-chain (Protocol LDP)
Remote Access Management

Remote Access Overview | 291
USB Modems for Remote Management of Security Devices | 319
Secure Web Access for Remote Management | 339
Example: Controlling Management Access on SRX Series Devices | 349
Configuration Guidelines for Securing Console Port Access | 354
Remote Access Overview

IN THIS SECTION

- System Services Overview | 291
- Configuring Telnet Service for Remote Access to a Router or Switch | 292
- Configuring FTP Service for Remote Access to the Router or Switch | 293
- Configuring Finger Service for Remote Access to the Router | 294
- Configuring SSH Service for Remote Access to the Router or Switch | 294
- The telnet Command | 298
- The ssh Command | 299
- Configuring SSH Host Keys for Secure Copying of Data | 300
- Configuring the SSH Service to Support Legacy Cryptography | 304
- Configuring Outbound SSH Service | 306
- Configuring NETCONF-Over-SSH Connections on a Specified TCP Port | 310
- Configuring Password Retry Limits for Telnet and SSH Access | 311
- Example: Configuring a Filter to Block Telnet and SSH Access | 312

You can access a router, switch, or security device remotely using DHCP, Finger, FTP, rlogin, SSH, and Telnet services and so on. This topic shows you how to configure remote access using Telnet, SSH, FTP, and Finger services. Read this topic for more information.

System Services Overview

For security reasons, remote access to the router is disabled by default. You must configure the router explicitly so that users on remote systems can access it. The router can be accessed from a remote system by means of the DHCP, finger, FTP, rlogin, SSH, and Telnet services. In addition, Junos XML protocol client applications can use Secure Sockets Layer (SSL) or the Junos XML protocol-specific clear-text service, among other services.
NOTE: To protect system resources, you can limit the number of simultaneous connections that a service accepts and the number of processes owned by a single user. If either limit is exceeded, connection attempts fail.

SEE ALSO

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
- DHCP Access Service Overview | 693
- Configuring the Router as an Extended DHCP Local Server | 723
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 725
- Configuring DTCP-over-SSH Service for the Flow-Tap Application
- Configuring TACACS+ System Accounting | 278

Configuring Telnet Service for Remote Access to a Router or Switch

To configure the router or switch to accept Telnet as an access service, include the `telnet` statement at the `[edit system services]` hierarchy level:

```plaintext
[edit system services]
telnet {
    connection-limit limit;
    rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous Telnet sessions and connection attempts per minute.

Optionally, you can include either or both of the following statements to change the defaults:

- `connection-limit limit`—Maximum number of simultaneous connections per protocol (IPV4 and IPv6).
  The range is from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of telnet sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 telnet sessions and 10 IPv4 telnet sessions.
• **rate-limit limit**—Maximum number of connection attempts accepted per minute (from 1 through 250).
  The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

You cannot include the `telnet` statement on devices that run the Junos-FIPS software. We recommend that you do not use Telnet in a Common Criteria environment.

**SEE ALSO**

| `telnet` | 2901 |

### Configuring FTP Service for Remote Access to the Router or Switch

To configure the router or switch to accept FTP as an access service, include the `ftp` statement at the `[edit system services]` hierarchy level:

```plaintext
[edit system services]
ftp {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router or switch supports a limited number of simultaneous FTP sessions and connection attempts per minute. You can include either or both of the following statements to change the defaults:

- **connection-limit limit**—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 FTP sessions and 10 IPv4 FTP sessions.

- **rate-limit limit**—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 FTP session connection attempts and 10 IPv4 FTP session connection attempts.

You can use passive FTP to access devices that accept only passive FTP services. All commands and statements that use FTP also accept passive FTP. Include the `ftp` statement at the `[edit system services]` hierarchy level to use either active FTP or passive FTP.

To start a passive FTP session, use `pasvftp` (instead of `ftp`) in the standard FTP format (`ftp://destination`). For example:
request system software add pasvftp://name.com/jinstall.tgz

You cannot include the `ftp` statement on routers or switches that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

## Configuring Finger Service for Remote Access to the Router

To configure the router to accept finger as an access service, include the `finger` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
finger {
  connection-limit limit;
  rate-limit limit;
}
```

By default, the router supports a limited number of simultaneous finger sessions and connection attempts per minute. Optionally, you can include either or both of the following statements to change the defaults:

- **connection-limit limit**—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 clear-text service sessions and 10 IPv4 clear-text service sessions.

- **rate-limit limit**—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 session connection attempts per minute and 10 IPv4 session connection attempts per minute.

You cannot include the `finger` statement on routers that run the Junos-FIPS software. We recommend that you do not use the finger service in a Common Criteria environment.

## Configuring SSH Service for Remote Access to the Router or Switch

**IN THIS SECTION**
- Configuring the Root Login Through SSH | 296
- Configuring the SSH Protocol Version | 296
To configure the router or switch to accept SSH as an access service, include the `ssh` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
ssh {
    authentication-order [method1 method2...];
    ciphers [cipher1 cipher2 cipher3 ...];
    client-alive-count-max seconds;
    client-alive-interval seconds;
    connection-limit limit;
    fingerprint-hash (md5 | sha2-256);
    hostkey-algorithm (algorithm | no-algorithm);
    key-exchange [algorithm1 algorithm2...];
    macs [algorithm1 algorithm2...];
    max-sessions-per-connection <number>;
    no-passwords;
    no-public-keys;
    no-tcp-forwarding;
    protocol-version [v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
}
```

By default, the router or switch supports a limited number of simultaneous SSH sessions and connection attempts per minute. Use the following statements to change the defaults:

- **connection-limit limit**—Maximum number of simultaneous connections per protocol (IPv4 and IPv6). The range is a value from 1 through 250. The default is 75. When you configure a connection limit, the limit is applicable to the number of SSH sessions per protocol (IPv4 and IPv6). For example, a connection limit of 10 allows 10 IPv6 SSH sessions and 10 IPv4 SSH sessions.

- **max-sessions-per-connection number**—Include this statement to specify the maximum number of SSH sessions allowed per single SSH connection. This allows you to limit the number of cloned sessions tunneled within a single SSH connection. The default value is 10.

- **rate-limit limit**—Maximum number of connection attempts accepted per minute (a value from 1 through 250). The default is 150. When you configure a rate limit, the limit is applicable to the number of
connection attempts per protocol (IPv4 and IPv6). For example, a rate limit of 10 allows 10 IPv6 SSH session connection attempts per minute and 10 IPv4 SSH session connection attempts per minute.

- **data-limit**—Data limit before renegotiating session keys (bytes)
- **time-limit**—Time limit before renegotiating session keys (minutes)

By default, a user can create an SSH tunnel over a CLI session to a router running Junos OS via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or access control lists allowing access to resources beyond the router. Use the `no-tcp-forwarding` option to prevent a user from creating an SSH tunnel to a router via SSH.

For information about other configuration settings, see the following topics:

### Configuring the Root Login Through SSH

By default, users are allowed to log in to the router or switch as **root** through SSH when the authentication method does not require a password. To control user access through SSH, include the `root-login` statement at the `[edit system services ssh]` hierarchy level:

```
[edit system services ssh]
root-login (allow | deny | deny-password);
```

- **allow**—Allows users to log in to the router or switch as root through SSH.
- **deny**—Disables users from logging in to the router or switch as root through SSH.
- **deny-password**—Allows users to log in to the router or switch as root through SSH when the authentication method (for example, RSA) does not require a password.

The default is **deny-password**.

### Configuring the SSH Protocol Version

By default, only version 2 of the SSH protocol is enabled.

To configure the router or switch to use version 2 of the SSH protocol, include the `protocol-version` statement and specify `v2` at the `[edit system services ssh]` hierarchy level:

```
[edit system services ssh]
protocol-version [ v2 ];
```

Systems in FIPS mode always use SSH protocol version v2.
Configuring the Client Alive Mechanism

The client alive mechanism is valuable when the client or server depends on knowing when a connection has become inactive. It differs from the standard keepalive mechanism because the client alive messages are sent through the encrypted channel. The client alive mechanism is not enabled at default. To enable it, configure the `client-alive-count-max` and `client-alive-interval` statements. This option applies to SSH protocol version 2 only.

In the following example, unresponsive SSH clients will be disconnected after approximately 100 seconds (20 x 5).

```bash
[edit system services ssh]
client-alive-count-max 5;
client-alive-interval 20;
```

SEE ALSO

| ssh | 2284 |

Configuring the SSH Fingerprint Hash Algorithm

To configure the hash algorithm used by the SSH server when it displays key fingerprints, include the `fingerprint-hash` statement and specify `md5` or `sha2-256` at the `[edit system services ssh]` hierarchy level:

```bash
[edit system services ssh]
fingerprint-hash (md5 | sha2-256);
```

The `md5` hash algorithm is unavailable on systems in FIPS mode.

SEE ALSO

| ssh | 2284 |
### The telnet Command

You can use the CLI `telnet` command to open a Telnet session to a remote device:

```
user@host> telnet host <8bit> <bypass-routing> <inet> <interface interface-name> <no-resolve> <port port> <routing-instance routing-instance-name> <source address>
```

**NOTE:** On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent Telnet sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

<table>
<thead>
<tr>
<th>Device</th>
<th>Max. Concurrent Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX100</td>
<td>3</td>
</tr>
<tr>
<td>SRX210</td>
<td>3</td>
</tr>
<tr>
<td>SRX220</td>
<td>5</td>
</tr>
<tr>
<td>SRX240</td>
<td>3</td>
</tr>
<tr>
<td>SRX300</td>
<td>3</td>
</tr>
<tr>
<td>SRX320</td>
<td>5</td>
</tr>
<tr>
<td>SRX340</td>
<td>5</td>
</tr>
<tr>
<td>SRX345</td>
<td>5</td>
</tr>
<tr>
<td>SRX1500</td>
<td>5</td>
</tr>
</tbody>
</table>

To exit the Telnet session and return to the Telnet command prompt, press Ctrl-].

To exit the Telnet session and return to the CLI command prompt, enter `quit`.

Table 17 on page 298 describes the `telnet` command options.

**Table 17: CLI telnet Command Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>8bit</code></td>
<td>Use an 8-bit data path.</td>
</tr>
<tr>
<td><code>bypass-routing</code></td>
<td>Bypass the routing tables and open a Telnet session only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Open a Telnet session to the specified hostname or IP address.</td>
</tr>
<tr>
<td><code>inet</code></td>
<td>Force the Telnet session to an IPv4 destination.</td>
</tr>
<tr>
<td><code>interface source-interface</code></td>
<td>Open a Telnet session to a host on the specified interface. If you do not include this option, all interfaces are used.</td>
</tr>
<tr>
<td><code>no-resolve</code></td>
<td>Suppress the display of symbolic names.</td>
</tr>
</tbody>
</table>
Table 17: CLI telnet Command Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port port</code></td>
<td>Specify the port number or service name on the host.</td>
</tr>
<tr>
<td><code>routing-instance</code></td>
<td>Use the specified routing instance for the Telnet session.</td>
</tr>
<tr>
<td><code>routing-instance-name</code></td>
<td></td>
</tr>
<tr>
<td><code>source address</code></td>
<td>Use the specified source address for the Telnet session.</td>
</tr>
</tbody>
</table>

The ssh Command

You can use the CLI `ssh` command to use the secure shell (SSH) program to open a connection to a remote device:

```
user@host> ssh host <bypass-routing> <inet> <interface interface-name> <routing-instance routing-instance-name> <source address> <v1> <v2>
```

**NOTE:** On SRX100, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the maximum number of concurrent SSH sessions is indicated in the following table. Platform support depends on the Junos OS release in your installation.

<table>
<thead>
<tr>
<th></th>
<th>SRX100</th>
<th>SRX210</th>
<th>SRX220</th>
<th>SRX240</th>
<th>SRX300</th>
<th>SRX320</th>
<th>SRX340</th>
<th>SRX345</th>
<th>SRX1500</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 18 on page 299 describes the `ssh` command options.

Table 18: CLI ssh Command Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bypass-routing</code></td>
<td>Bypass the routing tables and open an SSH connection only to hosts on directly attached interfaces. If the host is not on a directly attached interface, an error message is returned.</td>
</tr>
</tbody>
</table>
Table 18: CLI ssh Command Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>host</strong></td>
<td>Open an SSH connection to the specified hostname or IP address.</td>
</tr>
<tr>
<td><strong>inet</strong></td>
<td>Force the SSH connection to an IPv4 destination.</td>
</tr>
<tr>
<td><strong>interface source-interface</strong></td>
<td>Open an SSH connection to a host on the specified interface. If you do not include this option, all interfaces are used.</td>
</tr>
<tr>
<td><strong>routing-instance routing-instance-name</strong></td>
<td>Use the specified routing instance for the SSH connection.</td>
</tr>
<tr>
<td><strong>source address</strong></td>
<td>Use the specified source address for the SSH connection.</td>
</tr>
<tr>
<td><strong>v1</strong></td>
<td>Force SSH to use version 1 for the connection.</td>
</tr>
<tr>
<td><strong>v2</strong></td>
<td>Force SSH to use version 2 for the connection.</td>
</tr>
</tbody>
</table>

Configuring SSH Host Keys for Secure Copying of Data

Secure Shell (SSH) uses encryption algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (SCP) as an alternative to FTP for the background transfer of data such as configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
• Verify that the host key is authentic.
• Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

Tasks to configure SSH host keys for secure copying of data are:
1. Configuring SSH Known Hosts | 301
2. Configuring Support for SCP File Transfer | 302
3. Updating SSH Host Key Information | 302

Configuring SSH Known Hosts

To configure SSH known hosts, include the host statement, and specify hostname and host key options for trusted servers at the [edit security ssh-known-hosts] hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
  dsa-key key;
}
host archive-server-url {
  rsa-key key;
}
host server-with-ssh-version-1, ip-address {
  rsa1-key key;
}
```

Host keys are one of the following:

• **dsa-key key**—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
• **ecdsa-sha2-nistp256-key key**—Base64 encoded ECDSA-SHA2-NIST256 key.
• **ecdsa-sha2-nistp384-key key**—Base64 encoded ECDSA-SHA2-NIST384 key.
• **ecdsa-sha2-nistp521-key key**—Base64 encoded ECDSA-SHA2-NIST521 key.
• **ed25519-key key**—Base64 encoded ED25519 key.
• **rsa-key key**—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
• **rsa1-key key**—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.
Starting in Junos OS Release 18.3R1, the `ssh-dss` and `ssh-dsa` hostkey algorithms are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.

**Configuring Support for SCP File Transfer**

To configure a known host to support background SCP file transfers, include the `archive-sites` statement at the `[edit system archival configuration]` hierarchy level.

```
[edit system archival configuration]
archive-sites {
    scp://username:<password>@host:<port>/url-path;
}
```

**NOTE:** When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" "') and enclose the IPv6 host address in brackets ([ ]). For example, "scp://username:<password>@[host]<:port>/url-path";

Setting the `archive-sites` statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites "<scp-url-path>"
The authenticity of host <my-archive-server (<server-ip-address>)> can't be established. RSA key fingerprint is <ascii-text-key>. Are you sure you want to continue connecting (yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering `yes` at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

**Updating SSH Host Key Information**

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the `archival configuration archive-sites` statement at the `[edit system]` hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

1. **Retrieving Host Key Information Manually** | 303
2. **Importing Host Key Information from a File** | 303
Retrieving Host Key Information Manually

To manually retrieve SSH public host key information, use the `fetch-from-server` option with the `set security ssh-known-hosts` command. You must include a hostname attribute with the `set security ssh-known-hosts fetch-from-server` command to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

Importing Host Key Information from a File

To manually import SSH host key information from the known-hosts file located at `/var/tmp/known-hosts` on the server, include the `load-key-file` option with the `set security ssh-known-hosts` command. You must include the path to the `known-hosts` file with the `set security ssh-known-hosts load-key-file` command to specify the location from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

SEE ALSO

- Importing SSL Certificates for Junos XML Protocol Support
Configuring the SSH Service to Support Legacy Cryptography

Starting in Junos OS Release 16.1, the SSH server in Junos OS is based on OpenSSH 7 and defaults to a more secure set of ciphers and key-exchange algorithms. OpenSSH 7 omits some legacy cryptography.

**NOTE:** Lack of support for legacy cryptography in devices causes Junos Space device discovery to fail. To work around this issue, configure the device to support the 3des-cbc or blowfish-cbc cipher, or both, and the **dh-group1-sha1** key-exchange method. This issue does not affect devices running Junos OS with upgraded FreeBSD.

**NOTE:** See the OpenSSH 7 documentation at [https://www.openssh.com/](https://www.openssh.com/) for more information about these extensions.

Junos OS Release 16.1 supports the following set of ciphers by default:

- chacha20-poly1305@openssh.com
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

In Junos OS Release 16.1, the following ciphers are not supported by default, but you can configure your device to support them. They are listed from the most secure to the least secure:

- aes256-cbc
- aes192-cbc
- aes128-cbc
- 3des-cbc
- blowfish-cbc
- cast128-cbc
- arcfour256
- arcfour128
- arcfour
Junos OS Release 16.1 supports the following set of key-exchange methods by default:

- `curve25519-sha256`
- `ecdh-sha2-nistp256`
- `ecdh-sha2-nistp384`
- `ecdh-sha2-nistp521`
- `group-exchange-sha2`
- `dh-group14-sha1`

In Junos OS Release 16.1, the following key-exchange methods are not supported by default, but you can configure your device to support them:

- `group-exchange-sha1`
- `dh-group1-sha1`

To configure the SSH service to support legacy cryptography:

1. Add support for ciphers by using the `set system services ssh ciphers [ cipher 1 cipher 2 ... ]` command. We recommend that you add the ciphers to the end of the configuration list so that they are among the last options used. In the following example, the `3des-cbc` and `blowfish-cbc` ciphers are added to the default set:

   ```
   [edit system services ssh]
   user@device# set ciphers [ chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com 3des-cbc blowfish-cbc ]
   ```

2. Add support for key-exchange methods by using the `set system services ssh key-exchange [ method 1 method 2 ... ]` command. We recommend that you add the key-exchange methods to the end of the configuration list so that they are among the last options used. In the following example, the `dh-group1-sha1` key-exchange method is added to the default set:

   ```
   [edit system services ssh]
   user@device# set key-exchange [ curve25519-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 group-exchange-sha2 dh-group14-sha1 dh-group1-sha1 ]
   ```

**NOTE:** By configuring an ordered set of ciphers, key-exchange methods, or message authentication codes (MACs), the newly defined set is applied to both server and client commands. Changes to the defaults affect the `file copy` command when you use Secure Copy Protocol (SCP).
3. Commit the configuration:

```
[edit]
user@device# commit
```

SEE ALSO

- ciphers  | 1564
- key-exchange  | 1890
- macs  | 1933

### Configuring Outbound SSH Service

You can configure a device running the Junos OS to initiate a TCP/IP connection with a client management application that would be blocked if the client attempted to initiate the connection (for example, if the device is behind a firewall). The `outbound-ssh` command instructs the device to create a TCP/IP connection with the client management application and to forward the identity of the device. Once the connection is established, the management application acts as the client and initiates the SSH sequence, and the device acts as the server and authenticates the client.

**NOTE:** There is no initiation command with outbound SSH. Once outbound SSH is configured and committed, the device begins to initiate an outbound SSH connection based on the committed configuration. The device repeatedly attempts to create this connection until successful. If the connection between the device and the client management application is dropped, the device again attempts to create a new outbound SSH connection until successful. This connection is maintained until the outbound SSH stanza is removed from the configuration.

To configure the device for outbound SSH connections, include the `outbound-ssh` statement at the `[edit system services]` hierarchy level:

```
[edit system services outbound-ssh]
```

The following topics describe the tasks for configuring the outbound SSH service:

- Configuring the Device Identifier for Outbound SSH Connections  | 307
- Sending the Public SSH Host Key to the Outbound SSH Client  | 307
Configuring the Device Identifier for Outbound SSH Connections

Each time the device establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the device to the management client. Within this transmission is the value of `device-id`.

To configure the device identifier of the device, include the `device-id` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when `secret` is not configured:

```
MSG-ID: DEVICE-CONN-INFO
MSG-VER: V1
DEVICE-ID: <device-id>
```

Sending the Public SSH Host Key to the Outbound SSH Client

Each time the router or switch establishes an outbound SSH connection, it first sends an initiation sequence to the management client. This sequence identifies the router or switch to the management client. Within this transmission is the value of `device-id`.

To configure the device identifier of the router or switch, include the `device-id` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
device-id device-id;
```

The initiation sequence when `secret` is not configured:
During the initialization of an SSH connection, the client authenticates the identity of the device using the public SSH host key of the device. Therefore, before the client can initiate the SSH sequence, it needs the public SSH key of the device. When you configure the `secret` statement, the device passes its public SSH key as part of the outbound SSH connection initiation sequence.

When the `secret` statement is set and the device establishes an outbound SSH connection, the device communicates its device ID, its public SSH key, and an SHA1 hash derived in part from the `secret` statement. The value of the `secret` statement is shared between the device and the management client. The client uses the shared secret to authenticate the public SSH host key it is receiving to determine whether the public key is from the device identified by the `device-id` statement.

Using the `secret` statement to transport the public SSH host key is optional. You can manually transport and install the public key onto the client system.

**NOTE:** Including the `secret` statement means that the device sends its public SSH host key every time it establishes a connection to the client. It is then up to the client to decide what to do with the SSH host key if it already has one for that device. We recommend that you replace the client's copy with the new key. Host keys can change for various reasons and by replacing the key each time a connection is established, you ensure that the client has the latest key.

To send the router’s or switch’s public SSH host key when the device connects to the client, include the `secret` statement at the `[edit system services outbound-ssh client client-id]` hierarchy level:

```
[edit system services outbound-ssh client client-id]
secret password;
```

The following message is sent by the device when the `secret` attribute is configured:

```
MSG-ID: DEVICE-CONN-INFO
MSG-VER: V1
DEVICE-ID: <device-id>
HOST-KEY: <public-hot-key>
HMAC:<HMAC(pub-SSH-host-key, <secret>>)
```
Configuring Keepalive Messages for Outbound SSH Connections

Once the client application has the router’s or switch’s public SSH host key, it can then initiate the SSH sequence as if it had created the TCP/IP connection and can authenticate the device using its copy of the router’s or switch’s public host SSH key as part of that sequence. The device authenticates the client user through the mechanisms supported in the Junos OS (RSA/DSA public string or password authentication).

To enable the device to send SSH protocol keepalive messages to the client application, configure the keep-alive statement at the [edit system services outbound-ssh client client-id] hierarchy level:

```
[edit system services outbound-ssh client client-id]
keep-alive {
    retry number;
    timeout seconds;
}
```

Configuring a New Outbound SSH Connection

When disconnected, the device begins to initiate a new outbound SSH connection. To specify how the device reconnects to the server after a connection is dropped, include the reconnect-strategy statement at the [edit system services outbound-ssh client client-id] hierarchy level:

```
[edit system services outbound-ssh client client-id]
reconnect-strategy (sticky | in-order);
```

You can also specify the number of retry attempts and set the amount of time before the reconnection attempts stop. See "Configuring Keepalive Messages for Outbound SSH Connections" on page 309.

Configuring the Outbound SSH Client to Accept NETCONF as an Available Service

To configure the application to accept NETCONF as an available service, include the services netconf statement at the [edit system services outbound-ssh client client-id] hierarchy level:

```
[edit system services outbound-ssh client client-id]
services {
    netconf;
}
```
Configuring Outbound SSH Clients

To configure the clients available for this outbound SSH connection, list each client with a separate address statement at the [edit system services outbound-ssh client client-id] hierarchy level:

```
[edit system services outbound-ssh client client-id]
  address address [
    retry number;
    timeout seconds;
    port port-number;
  ]
```

NOTE: Outbound SSH connections support IPv4 and IPv6 address formats.

Configuring Routing Instances for Outbound SSH Clients

(SRX Series and MX Series only) Starting in Junos OS Release 19.3R1, you can specify the name of the routing instance on which the outbound SSH connectivity needs to be established by including the routing-instance statement at the [edit system services outbound-ssh] hierarchy level:

```
[edit system services outbound-ssh routing-instance routing-instance-name]
```

To use the management routing instance, first enable the mgmt_junos routing instance using the set system management-instance command.

To use any other routing instance, first configure the routing instance at the [edit routing-instances] hierarchy.

If you do not specify a routing instance, your device will establish the outbound SSH connection using the default routing table.

Configuring NETCONF-Over-SSH Connections on a Specified TCP Port

The Junos OS enables you to restrict incoming NETCONF connections to a specified TCP port without configuring a firewall. To configure the TCP port used for NETCONF-over-SSH connections, include the port statement at the [edit system services netconf ssh] hierarchy level. The configured port accepts only NETCONF-over-SSH sessions. Regular SSH session requests for this port are rejected.
You can either configure the default port 830 for NETCONF connections over SSH, as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*, or configure any port from 1 through 65535.

**NOTE:**

- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

**SEE ALSO**

- port (NETCONF) | 2073

---

### Configuring Password Retry Limits for Telnet and SSH Access

To prevent brute force and dictionary attacks, the device performs the following actions for Telnet or SSH sessions by default:

- Disconnects a session after a maximum of 10 consecutive password retries.
- After the second password retry, introduces a delay in multiples of 5 seconds between subsequent password retries.
  
  For example, the device introduces a delay of 5 seconds between the third and fourth password retry, a delay of 10 seconds between the fourth and fifth password retry, and so on.
- Enforces a minimum session time of 20 seconds during which a session cannot be disconnected.

  Configuring the minimum session time prevents malicious users from disconnecting sessions before the password retry delay goes into effect, and attempting brute force and dictionary attacks with multiple logins.

You can configure the password retry limits for Telnet and SSH access. In this example, you configure the device to take the following actions for Telnet and SSH sessions:

- Allow a maximum of four consecutive password retries before disconnecting a session.
- Introduce a delay in multiples of 5 seconds between password retries that occur after the second password retry.
• Enforce a minimum session time of 40 seconds during which a session cannot be disconnected.

To configure password retry limits for Telnet and SSH access:

1. Set the maximum number of consecutive password retries before a Telnet or SSH or telnet session is disconnected. The default number is 10, but you can set a number from 1 through 10.

   ```
   [edit system login retry-options]
   user@host# set tries-before-disconnect 4
   ```

2. Set the threshold number of password retries after which a delay is introduced between two consecutive password retries. The default number is 2, but you can specify a value from 1 through 3.

   ```
   [edit system login retry-options]
   user@host# set backoff-threshold 2
   ```

3. Set the delay (in seconds) between consecutive password retries after the threshold number of password retries. The default delay is in multiples of 5 seconds, but you can specify a value from 5 through 10 seconds.

   ```
   [edit system login retry-options]
   user@host# set backoff-factor 5
   ```

4. Set the minimum length of time (in seconds) during which a Telnet or SSH session cannot be disconnected. The default is 20 seconds, but you can specify an interval from 20 through 60 seconds.

   ```
   [edit system login retry-options]
   user@host# set minimum-time 40
   ```

5. If you are done configuring the device, enter `commit` from configuration mode.

---

**Example: Configuring a Filter to Block Telnet and SSH Access**

---

**IN THIS SECTION**

- Requirements | 313
- Overview | 313
Requirements

You must have access to a remote host that has network connectivity with this device.

Overview

In this example, you create an IPv4 stateless firewall filter that logs and rejects Telnet or SSH access packets unless the packet is destined for or originates from the 192.168.1.0/24 subnet.

- To match packets destined for or originating from the address 192.168.1.0/24 subnet, you use the source-address 192.168.1.0/24 IPv4 match condition.
- To match packets destined for or originating from a TCP port, Telnet port, or SSH port, you use the protocol tcp, port telnet, and telnet ssh IPv4 match conditions.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure this example, perform the following tasks:

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set firewall family inet filter local_acl term terminal_access from source-address 192.168.1.0/24
set firewall family inet filter local_acl term terminal_access from protocol tcp
set firewall family inet filter local_acl term terminal_access from port ssh
set firewall family inet filter local_acl term terminal_access from port telnet
set firewall family inet filter local_acl term terminal_access then accept
set firewall family inet filter local_acl term terminal_access_denied from protocol tcp
set firewall family inet filter local_acl term terminal_access_denied from port ssh
set firewall family inet filter local_acl term terminal_access_denied from port telnet
set firewall family inet filter local_acl term terminal_access_denied then log
set firewall family inet filter local_acl term default-term then accept
set interfaces lo0 unit 0 family inet filter input local_acl
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

Configure the Stateless Firewall Filter

Step-by-Step Procedure

To configure the stateless firewall filter that selectively blocks Telnet and SSH access:

1. Create the stateless firewall filter local_acl.

   ```
   [edit]
   user@myhost# edit firewall family inet filter local_acl
   ```

2. Define the filter term terminal_access.

   ```
   [edit firewall family inet filter local_acl]
   user@myhost# set term terminal_access from source-address 192.168.1.0/24
   user@myhost# set term terminal_access from protocol tcp
   user@myhost# set term terminal_access from port ssh
   user@myhost# set term terminal_access from port telnet
   user@myhost# set term terminal_access then accept
   ```

3. Define the filter term terminal_access_denied.

   ```
   [edit firewall family inet filter local_acl]
   user@myhost# set term terminal_access_denied from protocol tcp
   user@myhost# set term terminal_access_denied from port ssh
   ```
Apply the Firewall Filter to the Loopback Interface

Step-by-Step Procedure

- To apply the firewall filter to the loopback interface:

```
user@myhost# set term terminal_access_denied from port telnet
user@myhost# set term terminal_access_denied then log
user@myhost# set term terminal_access_denied then reject
user@myhost# set term default-term then accept
```

Confirm and Commit Your Candidate Configuration

Step-by-Step Procedure

To confirm and then commit your candidate configuration:

1. Confirm the configuration of the stateless firewall filter by entering the `show firewall` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show firewall
family inet {
  filter local_acl {
    term terminal_access {
      from {
        source-address {
          192.168.1.0/24;
        }
        protocol tcp;
        port [ssh telnet];
      }
      then accept;
    }
    term terminal_access_denied {
      from {
        protocol tcp;
        port [ssh telnet];
      }
    }
  }
}
```
then {
  log;
  reject;
}
}

2. Confirm the configuration of the interface by entering the `show interfaces` configuration mode command. If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@myhost# show interfaces
lo0 {
  unit 0 {
    family inet {
      filter {
        input local_acl;
      }
      source-address 127.0.0.1/32;
    }
  }
}
```

3. If you are done configuring the device, commit your candidate configuration.

```
[edit]
user@myhost# commit
```

Verification

IN THIS SECTION

- Verifying Accepted Packets | 317
- Verifying Logged and Rejected Packets | 318
Confirm that the configuration is working properly.

**Verifying Accepted Packets**

**Purpose**
Verify that the actions of the firewall filter terms are taken.

**Action**
1. Clear the firewall log on your router or switch.

   ```
   user@myhost> clear firewall log
   ```

2. From a host at an IP address within the 192.168.1.0/24 subnet, use the `ssh hostname` command to verify that you can log in to the device using only SSH. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

   ```
   user@host-A> ssh myhost
   ```

   ```
   user@myhost’s password:
   --- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
   ```

   ```
   % cli
   ```

   ```
   user@myhost>
   ```

3. From a host at an IP address within the 192.168.1.0/24 subnet, use the `telnet hostname` command to verify that you can log in to your router or switch using only Telnet. This packet should be accepted, and the packet header information for this packet should not be logged in the firewall filter log buffer in the Packet Forwarding Engine.

   ```
   user@host-A> telnet myhost
   ```

   ```
   Trying 192.168.249.71...
   Connected to myhost-fxp0.example.net.
   Escape character is ‘^]’.
   ```

   ```
   host (tty0)
   ```

   ```
   login: user
   ```

   ```
   Password:
   --- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
   ```
4. Use the `show firewall log` command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.

   `user@myhost>` show firewall log

**Verifying Logged and Rejected Packets**

**Purpose**
Verify that the actions of the firewall filter terms are taken.

**Action**
1. Clear the firewall log on your router or switch.

   `user@myhost>` clear firewall log

2. From a host at an IP address outside of the 192.168.1.0/24 subnet, use the `ssh hostname` command to verify that you cannot log in to the device using only SSH. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the Packet Forwarding Engine.

   `user@host-B` ssh myhost

   
   ssh: connect to host sugar port 22: Connection refused
   --- JUNOS 11.1-20101102.0 built 2010-11-02 04:48:46 UTC
   %

3. From a host at an IP address outside of the 192.168.1.0/24 subnet, use the `telnet hostname` command to verify that you can log in to the device using only Telnet. This packet should be rejected, and the packet header information for this packet should be logged in the firewall filter log buffer in the PFE.

   `user@host-B>` telnet myhost

   Trying 192.168.249.71...
   telnet: connect to address 192.168.187.3: Connection refused
telnet: Unable to connect to remote host
%

4. Use the `show firewall log` command to verify that the routing table on the device does not contain any entries with a source address in the 192.168.1.0/24 subnet.
user@myhost> show firewall log

<table>
<thead>
<tr>
<th>Time</th>
<th>Filter</th>
<th>Action</th>
<th>Interface</th>
<th>Protocol</th>
<th>Src Addr</th>
<th>Dest Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>18:41:25</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>18:41:25</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>18:41:25</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>18:43:06</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>18:43:06</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>18:43:06</td>
<td>local_acl</td>
<td>R</td>
<td>fxp0.0</td>
<td>TCP</td>
<td>192.168.187.5</td>
<td>192.168.187.1</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3R1</td>
<td>Starting in Junos OS Release 18.3R1, the ssh-dss and ssh-dsa hostkey algorithms are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- USB Modems for Remote Management of Security Devices | 319
- Secure Web Access for Remote Management | 339

USB Modems for Remote Management of Security Devices

IN THIS SECTION

- USB Modem Interface Overview | 320
- USB Modem Configuration Overview | 323
- Example: Configuring a USB Modem Interface | 326
- Example: Configuring a Dialer Interface | 329
Junos OS allows the use of USB modems for remote management on SRX Series device. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. For more information, read this topic.

**USB Modem Interface Overview**

Juniper Networks SRX Series devices support the use of USB modems for remote management. You can use Telnet or SSH to connect to the device from a remote location through two modems over a telephone network. The USB modem is connected to the USB port on the device, and a second modem is connected to a remote management device such as a PC or laptop computer.

**NOTE:** USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, SRX345, SRX550HM devices.

You can configure your device to fail over to a USB modem connection when the primary Internet connection experiences interruption.

A USB modem connects to a device through modem interfaces that you configure. The device applies its own modem AT commands to initialize the attached modem. Modem setup requires that you connect and configure the USB modem at the device and the modem at the user end of the network.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem and its supporting dialer interfaces.

**NOTE:** Low-latency traffic such as VoIP traffic is not supported over USB modem connections.
NOTE: We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

USB Modem Interfaces

You configure two types of interfaces for USB modem connectivity:

- A physical interface which uses the naming convention `umd0`. The device creates this interface when a USB modem is connected to the USB port.

- A logical interface called the dialer interface. You use the dialer interface, `dln`, to configure dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP). You can configure multiple dialer interfaces for different functions on the device. After configuring the dialer interface, you must configure a backup method such as a dialer backup, a dialer filter, or a dialer watch.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface. Dialer pool priority has a range from 1 to 255, with 1 designating the lowest priority interfaces and 255 designating the highest priority interfaces.

Dialer Interface Rules

The following rules apply when you configure dialer interfaces for USB modem connections:

- The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.

- The dialer interface cannot be configured as a constituent link in a multilink bundle.

- The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
  - As a backup interface—for one primary interface
  - As a dialer filter
  - As a dialer watch interface
The backup dialer interfaces are activated only when the primary interface fails. USB modem backup connectivity is supported on all interfaces except lsq-0/0/0.

The dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an "interesting packet" arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed. You define an interesting packet using the dialer filter feature of the device. To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route. If the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

**How the Device Initializes USB Modems**

When you connect the USB modem to the USB port on the device, the device applies the modem AT commands configured in the **init-command-string** command to the initialization commands on the modem.

If you do not configure modem AT commands for the **init-command-string** command, the device applies the following default sequence of initialization commands to the modem: **AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0**. Table 19 on page 322 describes the commands. For more information about these commands, see the documentation for your modem.

**Table 19: Default Modem Initialization Commands**

<table>
<thead>
<tr>
<th>Modem Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>Attention. Informs the modem that a command follows.</td>
</tr>
<tr>
<td>S7=45</td>
<td>Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.</td>
</tr>
<tr>
<td>S0=0</td>
<td>Disables the auto answer feature, whereby the modem automatically answers calls.</td>
</tr>
<tr>
<td>V1</td>
<td>Displays result codes as words.</td>
</tr>
<tr>
<td>&amp;C1</td>
<td>Disables reset of the modem when it loses the carrier signal.</td>
</tr>
<tr>
<td>E0</td>
<td>Disables the display on the local terminal of commands issued to the modem from the local terminal.</td>
</tr>
<tr>
<td>Q0</td>
<td>Enables the display of result codes.</td>
</tr>
<tr>
<td>&amp;Q8</td>
<td>Enables Microcom Networking Protocol (MNP) error control mode.</td>
</tr>
</tbody>
</table>
Table 19: Default Modem Initialization Commands (continued)

<table>
<thead>
<tr>
<th>Modem Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%C0</td>
<td>Disables data compression.</td>
</tr>
</tbody>
</table>

When the device applies the modem AT commands in the `init-command-string` command or the default sequence of initialization commands to the modem, it compares them to the initialization commands already configured on the modem and makes the following changes:

- If the commands are the same, the device overrides existing modem values that do not match. For example, if the initialization commands on the modem include \( S0=0 \) and the device’s `init-command-string` command includes \( S0=2 \), the device applies \( S0=2 \).
- If the initialization commands on the modem do not include a command in the device’s `init-command-string` command, the device adds it. For example, if the `init-command-string` command includes the command `L2`, but the modem commands do not include it, the device adds `L2` to the initialization commands configured on the modem.

**NOTE:** On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), keepalives do not get exchanged, and the interface goes down. (Platform support depends on the Junos OS release in your installation.)

### USB Modem Configuration Overview

**NOTE:** USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, and SRX345 devices.

Before you begin:

1. **Install device hardware.** For more information, see the Getting Started Guide for your device.
2. **Establish basic connectivity.** For more information, see the Getting Started Guide for your device.
4. Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.

5. Connect the USB modem to the device's USB port.

   **NOTE:** When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

   a. Plug the modem into the USB port.

   b. Connect the modem to your telephone network.

Suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. This example shows you how to establish a backup connection between the branch office and head office routers. See Table 20 on page 324 for a summarized description of the procedure.

**Table 20: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity**

<table>
<thead>
<tr>
<th>Router Location</th>
<th>Configuration Requirement</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Office</td>
<td>Configure the logical dialer interface on the branch office router for USB modem dial backup.</td>
<td>To configure the logical dialer interface, see &quot;Example: Configuring a USB Modem Interface&quot; on page 326.</td>
</tr>
<tr>
<td></td>
<td>Configure the dialer interface dl0 on the branch office router using one of the following backup methods:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure the dialer interface dl0 as the backup interface on the branch office router's primary T1 interface t1-1/0/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure a dialer filter on the branch office router's dialer interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configure a dialer watch on the branch office router's dialer interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure the dialer interface dl0 on the branch office router using one of the following backup methods:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To configure dl0 as a backup for t1-1/0/0 see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To configure a dialer filter on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To configure a dialer watch on dl0, see Example: Configuring Dialer Interfaces and Backup Methods for USB Modem Dial Backup.</td>
<td></td>
</tr>
</tbody>
</table>
Table 20: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity (continued)

<table>
<thead>
<tr>
<th>Router Location</th>
<th>Configuration Requirement</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office</td>
<td>Configure dial-in on the dialer interface dl0 on the head office router.</td>
<td>To configure dial-in on the head office router, see “Example: Configuring a Dialer Interface for USB Modem Dial-In” on page 334.</td>
</tr>
</tbody>
</table>

If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085321091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

See Table 21 on page 325 for a list of available incoming map options.

Table 21: Incoming Map Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-all</td>
<td>Dialer interface accepts all incoming calls. You can configure the accept-all option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the accept-all option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.</td>
</tr>
<tr>
<td>caller</td>
<td>Dialer interface accepts calls from a specific caller ID. You can configure a maximum of 15 caller IDs per dialer interface. The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.</td>
</tr>
</tbody>
</table>

You configure dialer interfaces to support PAP. PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair are repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.
Example: Configuring a USB Modem Interface

This example shows how to configure a USB modem interface for dial backup.

NOTE: USB modems are no longer supported for dial backup on SRX300, SRX320, SRX340, and SRX345 devices.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you create an interface called as umd0 for USB modem connectivity and set the dialer pool priority to 25. You also configure a modem initialization string to autoanswer after a specified number of rings. The default modem initialization string is \texttt{AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0}. The modem command \texttt{S0=0} disables the modem from autoanswering the calls. Finally, you set the modem to act as a dial-in WAN backup interface.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the command into the CLI at the [edit] hierarchy level, and then enter \texttt{commit} from configuration mode.

\begin{verbatim}
set interfaces umd0 dialer-options pool usb-modem-dialer-pool priority 25
\end{verbatim}
**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure a USB modem interface for dial backup:

1. Create an interface.

   ```
   [edit]
   user@host# edit interfaces umd0
   ```

2. Set the dialer options and priority.

   ```
   [edit interfaces umd0]
   user@host# set dialer-options pool usb-modem-dialer-pool priority 25
   ```

3. Specify the modem options.

   ```
   [edit interfaces umd0]
   user@host# set modem-options init-command-string "ATS0=2 \n"
   ```

4. Set the modem to act as a dial-in WAN backup interface.

   ```
   [edit interfaces umd0]
   user@host# set modem-options dialin routable
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show interface umd0` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interface umd0
modem-options {
  init-command-string "ATS0=2 \n";
  dialin routable;
}
```
dialer-options {
    pool usb-modem-dialer-pool priority 25;
}

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

Confirm that the configuration is working properly.

**Verifying the Configuration**

**Purpose**
Verify a USB modem interface for dial backup.

**Action**
From configuration mode, enter the `show interfaces umd0 extensive` command. The output shows a summary of interface information and displays the modem status.

Physical interface: umd0, Enabled, Physical link is Up
Interface index: 64, SNMP ifIndex: 33, Generation: 1
    Type: Async-Serial, Link-level type: PPP-Subordinate, MTU: 1504,
    Clocking: Unspecified, Speed: MODEM
    Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
    Link flags : None
    Hold-times : Up 0 ms, Down 0 ms
    Last flapped : Never
    Statistics last cleared: Never
Traffic statistics:
    Input bytes : 21672
    Output bytes : 22558
    Input packets: 1782
    Output packets: 1832
    Input errors:
        Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
    Resource errors: 0
    Output errors:
        Carrier transitions: 63, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
    MODEM status:
        Modem type : LT V.92 1.0 MT56342BA-USB-V92 Data/Fax Modem
Example: Configuring a Dialer Interface

IN THIS SECTION

- Requirements | 329
- Overview | 330
- Configuration | 330
- Verification | 332

This example shows how to configure a logical dialer interface for an SRX300, SRX320, SRX340, or SRX345 device.

Requirements

Before you begin:

- Install device hardware and establish basic connectivity. See the Getting Started Guide for your device.
- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637, from US Robotics (http://www.usr.com/).
- Order a dial-up modem for the PC or laptop computer at the remote location from where you want to connect to the device.
- Order a PSTN line from your telecommunications service provider. Contact your service provider.
Overview

In this example, you configure a logical dialer interface called dl0 to establish USB connectivity. You can configure multiple dialer interfaces for different functions on the device. You add a description to differentiate among different dialer interfaces. For example, this modem is called USB-modem-remote-management. Configure PPP encapsulation and set the logical unit as 0. You then specify the name of the dialer pool as usb-modem-dialer-pool and set the source and destination IP addresses as 172.20.10.2, and 172.20.10.1, respectively.

NOTE: You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.

NOTE: If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the USB modem call is mapped.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set interfaces dl0 description USB-modem-remote-management encapsulation ppp
set interfaces dl0 unit 0 dialer-options pool usb-modem-dialer-pool
set interfaces dl0 unit 0 family inet address 172.20.10.2 destination 172.20.10.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure a logical dialer interface for the device:

1. Create an interface.
2. Add a description and configure PPP encapsulation.

```
[edit interfaces dl0]
user@host# set description USB-modem-remote-management
user@host# set encapsulation ppp
```

3. Create the logical unit.

NOTE: The logical unit number must be 0.

```
[edit interfaces dl0]
user@host# set unit 0
```

4. Configure the name of the dialer pool to use for USB modem connectivity.

```
[edit interfaces dl0 unit 0]
user@host# set dialer-options pool usb-modem-dialer-pool
```

5. Configure source and destination IP addresses for the dialer interface.

```
[edit interfaces dl0 unit 0]
user@host# set family inet address 172.20.10.2 destination 172.20.10.1
```

**Results**

From configuration mode, confirm your configuration by entering the `show interfaces dl0` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces dl0
description USB-modem-remote-management;
   encapsulation ppp;
unit 0 {
```
family inet {
  address 172.20.10.2/32 {
    destination 172.20.10.1;
  }
}
dialer-options {
  pool usb-modem-dialer-pool;
}

If you are done configuring the device, enter **commit** from configuration mode.

**Verification**

Confirm that the configuration is working properly.

**Verifying a Dialer Interface**

**Purpose**
Verify that the dialer interface has been configured.

**Action**
From configuration mode, enter the **show interfaces dl0 extensive** command. The output shows a summary of dialer interface information.

Physical interface: dl0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 129
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed: Unspecified
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Link flags : Keepalives
  Physical info : Unspecified
  Hold-times : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input  bytes : 13859  0 bps
    Output bytes : 0 0 bps
    Input  packets: 317 0 pps
    Output packets: 0 0 pps
Logical interface dl0.0 (Index 70) (SNMP ifIndex 75) (Generation 146)
Description: USB-modem-remote-management
Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP
Dialer:
  State: Active, Dial pool: usb-modem-dialer-pool
  Dial strings: 220
  Subordinate interfaces: umd0 (Index 64)
  Activation delay: 0, Deactivation delay: 0
  Initial route check delay: 120
  Redial delay: 3
  Callback wait period: 5
  Load threshold: 0, Load interval: 60
Bandwidth: 115200
Traffic statistics:
  Input bytes : 24839
  Output bytes : 17792
  Input packets: 489
  Output packets: 340
Local statistics:
  Input bytes : 10980
  Output bytes : 17792
  Input packets: 172
  Output packets: 340
Transit statistics:
  Input bytes : 13859
  Output bytes : 0
  Input packets: 317
  Output packets: 0
LCP state: Opened
CHAP state: Success
Protocol inet, MTU: 1500, Generation: 136, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Example: Configuring a Dialer Interface for USB Modem Dial-In

IN THIS SECTION

- Requirements | 334
- Overview | 334
- Configuration | 335
- Verification | 336

This example shows how to configure a dialer interface for USB modem dial-in.

NOTE: USB modems are no longer supported for dial-in to a dialer interface on SRX300, SRX320, SRX340, and SRX345 devices.

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

To enable connections to the USB modem from a remote location, you must configure the dialer interfaces set up for USB modem use to accept incoming calls. You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.

If the dialer interface is configured to accept only calls from a specific caller ID, the system matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call's caller ID has more digits than the configured caller IDs, the system performs a right-to-left match of the incoming call's caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call's caller ID is 4085550115 and the caller ID
configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

You can configure the following incoming map options for the dialer interface:

- **accept-all**—Dialer interface accepts all incoming calls.
  
  You can configure the **accept-all** option for only one of the dialer interfaces associated with a USB modem physical interface. The device uses the dialer interface with the **accept-all** option configured only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.

- **caller**—Dialer interface accepts calls from a specific caller ID— for example, **4085550115**. You can configure a maximum of 15 caller IDs per dialer interface.
  
  The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.

In this example, you configure the incoming map option as caller 4085550115 for dialer interface dl0.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the command into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
set interfaces dl0 unit 0 dialer-options incoming-map caller 4085550115
```

**Step-by-Step Procedure**

To configure a dialer interface for USB modem dial-in:

1. Select a dialer interface.

   ```
   [edit]
   user@host# edit interfaces dl0
   ```

2. Configure the incoming map options.

   ```
   [edit]
   user@host# edit unit 0 dialer-options incoming-map caller 4085551515
   ```

3. If you are done configuring the device, commit the configuration.
Verification

To verify the configuration is working properly, enter the `show interface dl0` command.

### Configuring a Dial-Up Modem Connection Remotely

To remotely connect to the USB modem connected to the USB port on the device, you must configure a dial-up modem connection on the PC or laptop computer at your remote location. Configure the dial-up modem connection properties to disable IP header compression.

To configure a dial-up modem connection remotely:

1. At your remote location, connect a modem to a management device such as a PC or laptop computer.

2. Connect the modem to your telephone network.


4. Click `Create a new connection`. The New Connection Wizard appears.

5. Click `Next`. The New Connection Wizard: Network Connection Type page appears.

6. Select `Connect to the network at my workplace`, and then click `Next`.
   The New Connection Wizard: Network Connection page appears.

7. Select `Dial-up connection`, and then click `Next`. The New Connection Wizard: Connection Name page appears.

8. In the Company Name box, type the dial-up connection name, for example `USB-modem-connect`. Then, click `Next`. The New Connection Wizard: Phone Number to Dial page appears.

9. In the Phone number box, type the telephone number of the PSTN line connected to the USB modem at the device end.
10. Click **Next** twice, and then click **Finish**. The Connect USB-modem-connect page appears.

11. If CHAP is configured on the dialer interface used for the USB modem interface at the device end, type the username and password configured in the CHAP configuration in the User name and Password boxes.

12. Click **Properties**. The USB-modem-connect Properties page appears.

13. In the Networking tab, select **Internet Protocol (TCP/IP)**, and then click **Properties**. The Internet Protocol (TCP/IP) Properties page appears.

14. Click **Advanced**. The Advanced TCP/IP Settings page appears.

15. Clear the **Use IP header compression** check box.

---

**Connecting to the Device Remotely**

To remotely connect to the device through a USB modem connected to the USB port on the device:

1. On the PC or laptop computer at your remote location, select **Start>Settings>Control Panel>Network Connections**. The Network Connections page appears.

2. Double-click the **USB-modem-connect** dial-up connection. The Connect USB-modem-connect page appears.

3. Click **Dial** to connect to the Juniper Networks device.

   When the connection is complete, you can use Telnet or SSH to connect to the device.

---

**Modifying USB Modem Initialization Commands**

**NOTE:** These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, see the documentation for your modem and enter equivalent modem commands. Applies to SRX300, SRX320, SRX340, SRX345 devices.
You can use the CLI configuration editor to override the value of an initialization command configured on the USB modem or configure additional commands for initializing USB modems.

NOTE: If you modify modem initialization commands when a call is in progress, the new initialization sequence is applied on the modem only when the call ends.

You can configure the following modem AT commands to initialize the USB modem:

- The command **S0=2** configures the modem to automatically answer calls on the second ring.
- The command **L2** configures medium speaker volume on the modem.

You can insert spaces between commands.

When you configure modem commands in the CLI configuration editor, you must follow these conventions:

- Use the newline character \n to indicate the end of a command sequence.
- Enclose the command string in double quotation marks.

You can override the value of the **S0=0** command in the initialization sequence configured on the modem and add the **L2** command.

To modify the initialization commands on a USB modem:

1. Configure the modem AT commands to initialize the USB modem.

   ```
   [edit interfaces umd0]
   user@host# set modem-options init-command-string "AT S0=2 L2 \n"
   ```

2. If you are done configuring the device, enter **commit** from configuration mode.

### Resetting USB Modems

For SRX300, SRX320, SRX340, and SRX345 devices, if the USB modem does not respond, you can reset the modem.

CAUTION: If you reset the modem when a call is in progress, the call is terminated.

To reset the USB modem, in operational mode, enter the following command:
You can manage a Juniper Networks device remotely through the J-Web interface. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports on the device as needed. Read this topic for information.
Secure Web Access Overview

You can manage a Juniper Networks device remotely through the J-Web interface. To communicate with the device, the J-Web interface uses the Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the device by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the Juniper Networks devices support HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The Juniper Networks device uses the Secure Sockets Layer (SSL) protocol to provide secure device management through the Web interface. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the device through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or the certificate has expired, you cannot access the device through HTTPS.

Without SSL encryption, communication between your device and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

HTTP access is enabled by default on the built-in management interfaces. By default, HTTPS access is supported on any interface with an SSL server certificate.

SEE ALSO

Configuring Device Addresses (IPv4 and Loopback Addresses)

Generating SSL Certificates for Secure Web Access (SRX Series Devices)

To generate an SSL certificate using the openssl command:

1. Enter openssl in the CLI. The openssl command generates a self-signed SSL certificate in privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   NOTE: Run this command on a LINUX or UNIX device because Juniper Networks Services Gateways do not support the openssl command.
Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following `openssl` command in your SSH command-line interface on a BSD or Linux system on which `openssl` is installed. The `openssl` command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   ```
   % openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
   ```

   where `filename` is the name of a file in which you want the SSL certificate to be written—for example, `my-certificate.pem`.

2. When prompted, type the appropriate information in the identification form. For example, type `US` for the country name.

3. Display the contents of the file that you created.

   ```
   cat my-certificate.pem
   ```

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.
You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```

SEE ALSO

- Configuring Management Access for the EX Series Switch (J-Web Procedure)
- Overview of Port Security

### Generating a Self-Signed SSL Certificate Automatically

To generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.

2. Reboot the system. The self-signed certificate is automatically generated at bootup time.

   ```
   user@host> request system reboot
   Reboot the system ? [yes,no] yes
   ```

3. Specify `system-generated-certificate` under HTTPS Web management.

   ```
   [edit]
   user@host# show system services web-management https system-generated-certificate
   ```

### Manually Generating Self-Signed SSL Certificates

To manually generate a self-signed SSL certificate on Juniper Networks devices:

1. Establish basic connectivity.

2. If you have root login access, you can manually generate the self-signed certificate by using the following commands:
### root@host> request security pki generate-key-pair size 512 certificate-id certname

Generated key pair sslcert, key size 512 bits

### root@host> request security pki local-certificate generate-self-signed certificate-id cert-name email email domain-name domain name ip-address IP address subject "DC= Domain name, CN= Common-Name, OU= Organizational-Unit-name, O= Organization-Name, ST= state, C= Country"

Self-signed certificate generated and loaded successfully

**NOTE:** When generating the certificate, you must specify the subject, e-mail address, and either domain-name or ip-address.

3. To verify that the certificate was generated and loaded properly, enter the `show security pki local-certificate` operational command and specify `local-certificate` under HTTPS Web management.

[edit]

```
root@host# show system services web-management https local-certificate certname
```

## Deleting Self-Signed Certificates (CLI Procedure)

You can delete a self-signed certificate that is automatically or manually generated from the EX Series switch. When you delete the automatically generated self-signed certificate, the switch generates a new self-signed certificate and stores it in the file system.

- To delete the automatically generated certificate and its associated key pair from the switch:

  ```
  user@switch> clear security pki local-certificate system-generated
  ```

- To delete a manually generated certificate and its associated key pair from the switch:

  ```
  user@switch> clear security pki local-certificate certificate-id certificate-id-name
  ```
To delete all manually generated certificates and their associated key pairs from the switch:

```
user@switch> clear security pki local-certificate all
```

## Understanding Self-Signed Certificates on EX Series Switches

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.

### NOTE:
Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.

The switches provide two methods for generating a self-signed certificate:

- **Automatic generation**

  In this case, the creator of the certificate is the switch. An automatically generated (also called "system-generated") self-signed certificate is configured on the switch by default.

  After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

  A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a `request system snapshot` command is issued.

  The switch uses the following distinguished name for the automatically generated certificate:

  "CN=<device serial number>, CN=system generated, CN=self-signed"

  If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- **Manual generation**

  In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.
Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

**Manually Generating Self-Signed Certificates on Switches (CLI Procedure)**

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

**Generating a Public-Private Key Pair on Switches**

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```

**NOTE:** Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.
After the public-private key pair is generated, the switch displays the following:

```
  generated key pair certificate-id-name, key size 1024 bits
```

### Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id certificate-id-name
domain-name domain-name email email-address ip-address switch-ip-address subject
subject-of-distinguished-name
```

The certificate you have generated is stored in the switch's file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the `show security pki local-certificate` operational command.

### SEE ALSO

- *Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)*

### Example: Configuring Secure Web Access

**IN THIS SECTION**

- Requirements | 347
- Overview | 347
- Configuration | 347
- Verification | 348
This example shows how to configure secure Web access on your device.

**Requirements**

No special configuration beyond device initialization is required before configuring this feature.

**NOTE:** You can enable HTTPS access on specified interfaces. If you enable HTTPS without specifying an interface, HTTPS is enabled on all interfaces.

**Overview**

In this example, you import the SSL certificate that you have generated as a new and private key in PEM format. You then enable HTTPS access and specify the SSL certificate to be used for authentication. Finally, you specify the port as 8443 on which HTTPS access is to be enabled.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set security certificates local new load-key-file /var/tmp/new.pem
set system services web-management https local-certificate new port 8443
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure secure Web access on your device:

1. Import the SSL certificate and private key.

   ```
   [edit security]
   user@host# set certificates local new load-key-file /var/tmp/new.pem
   ```

2. Enable HTTPS access and specify the SSL certificate and port.

   ```
   [edit system]
   ```
Results
From configuration mode, confirm your configuration by entering the show security command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security
certificates {
    local {
        new {
            "-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC/C5UI4frNqbiqPwbTiOkJvqoDw2YgYseOZ5zzVJyErgSg954T\n/euHM67Ck8hA0rcnb0YO+SY
Y5rCXLf4+2s8k9EypLtYRw/Ts66DZoXl4viqE7HSSsKn5sQw/UDBlw7/MJ+OpA ...
KYIf4CbbjIMMQI0HfudW6iSVBslONkzX+FT\ni95ddka6ilRnArEb4VFCR+e1QBdp1UjziYf7NuzDx4Z\n-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDgDCCAvWgAwIBAgIBADANBgkqhkiG9w0BAQ...</n

FADCBkJTELMAkGA1UEBhMCdXMx\nCzAJBgNVBAgTAmNhMRIwEAYDVQQHEwIwldW5ueHB1YnMxDTALBgNVBAMTBGFydWl...</n

fUYAnBYmsYWOH\n
-----END CERTIFICATE-----
"; ##SECRET-DATA
```

If you are done configuring the device, enter commit from configuration mode.

Verification

IN THIS SECTION
- Verifying an SSL Certificate Configuration | 348
- Verifying a Secure Access Configuration | 349

Confirm that the configuration is working properly.

Verifying an SSL Certificate Configuration

Purpose
Verify the SSL certificate configuration.

**Action**
From operational mode, enter the `show security` command.

**Verifying a Secure Access Configuration**

**Purpose**
Verify the secure access configuration.

**Action**
From operational mode, enter the `show system services` command. The following sample output displays the sample values for secure Web access:

```
[edit]
user@host# show system services
web-management {
  http;
  https {
    port 8443;
    local-certificate new;
  }
}
```

**RELATED DOCUMENTATION**

- Remote Access Overview | 291
- Junos OS User Authentication Overview | 209

**Example: Controlling Management Access on SRX Series Devices**

**IN THIS SECTION**

- Requirements | 350
- Overview | 350
This example shows how to limit the management access to the specific IP addresses on an SRX Series devices to manage the device.

**Requirements**

No special configuration beyond device initialization is required before configuring this feature.

**Overview**

To limit the IP addresses that can manage a device, you can configure a firewall filter. This firewall filters must include a term to deny all traffic except the IP address that you allow to manage the device. You must apply the firewall filter to the loopback interface (lo0) as this ensures that only management traffic (traffic to the device) is filtered.

In this example you:

- Configure a prefix-list called `manager-ip`. This list defines a set of IP addresses that are allowed to manage the SRX Series device.
- Configure a firewall filter `FILTER1` that rejects all requesters except IP addresses available in the `manager-ip` prefix list. In this way, you are ensuring that IP address list specified in the prefix list can manage the device.
- Apply `FILTER1` filter to the loopback interface. Any time a packet hits any of the interfaces on the device, the loopback interface applies the filter `FILTER1`.

**Configuration**

Configuring an IP Address List to Restrict Management Access to a Device

**CLI Quick Configuration**
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set policy-options prefix-list manager-ip 192.168.4.254/32
set policy-options prefix-list manager-ip 10.0.0.0/8
set firewall filter FILTER1 term block_non_manager from source-address 0.0.0.0/0
set firewall filter FILTER1 term block_non_manager from source-prefix-list manager-ip except
set firewall filter FILTER1 term block_non_manager from protocol tcp
set firewall filter FILTER1 term block_non_manager from destination-port ssh
set firewall filter FILTER1 term block_non_manager from destination-port https
set firewall filter FILTER1 term block_non_manager from destination-port telnet
set firewall filter FILTER1 term block_non_manager from destination-port http
set firewall filter FILTER1 term block_non_manager then discard
set firewall filter FILTER1 term accept_everything_else then accept
set interfaces lo0 unit 0 family inet filter input FILTER1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

1. Define a set of allowed host addresses in the prefix list.

   ```
   [edit policy-options]
   user@host# set prefix-list manager-ip 192.168.4.254/32
   user@host# set prefix-list manager-ip 10.0.0.0/8
   ```

   **NOTE:** The configured list is referenced in the actual filter, where you can change your defined set of addresses.

2. Configure a firewall filter to deny traffic from all IP addresses except the IP addresses defined in the prefix list.

   ```
   [edit firewall filter]
   user@host# set manager-ip term block_non_manager from source-address 0.0.0.0/0
   user@host# set manager-ip term block_non_manager from source-prefix-list manager-ip except
   user@host# set manager-ip term block_non_manager from protocol tcp
   user@host# set manager-ip term block_non_manager from destination-port ssh
   user@host# set manager-ip term block_non_manager from destination-port https
   user@host# set manager-ip term block_non_manager from destination-port telnet
   ```
Management traffic that uses any of the listed destination ports is rejected when the traffic comes from an address in the list.

3. Configure a default term that accepts all other traffic.

```bash
[edit firewall filter]
user@host# set manager-ip term accept_everything_else then accept
```

4. Apply stateless firewall filters to the loopback interface to filter the packets originating from the hosts to which you are granting management access.

```bash
[edit interfaces lo0 unit 0 ]
user@host# set family inet filter input manager-ip
```

This configuration applies to traffic terminating at the device itself. If you have IPsec traffic, or OSPF, RIP, BGP, or any other traffic that terminates at the interface of the device, then you must add the IP address of the interface to the prefix list.

**Results**

From configuration mode, confirm your configuration by entering `show configuration` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```bash
user@host# show configuration policy-options
  prefix-list manager-ip {}
  10.0.0.0/8;
  192.168.4.254/32;
}
```

```bash
user@host# show configuration firewall
  filter FILTER1 {
  term block_non_manager {
    from {
      source-address {
        0.0.0.0/0;
      }
      source-prefix-list {
```
manager-ip except;
}
protocol tcp;
destination-port [ ssh https telnet http ];
}
then {
discard;
}
term accept_everything_else {
then accept;
}
}

If you are done configuring the device, enter commit from configuration mode.

### Verification

Confirm that the configuration is working properly.
Verifying Interfaces

Purpose
Verify if the interfaces are configured correctly.

Action
From operational mode, enter the following commands:

- show policy-options
- show firewall
- show interfaces

Related Documentation

Configuration Guidelines for Securing Console Port Access

Configuration Guidelines for Securing Console Port Access

In This Section

- Securing Console Port | 354
- Securing Mini-USB Ports | 356

We recommend disabling the console port to prevent unauthorized access to the device.

Securing Console Port

You can use the console port on the device to connect to the device through an RJ-45 serial cable. From the console port, you can use the CLI to configure the device. By default, the console port is enabled. To secure the console port, you can configure the device to take the following actions:
• Log out of the console session when you unplug the serial cable connected to the console port.
• Disable root login connections to the console. This action prevents a non-root user from performing password recovery operation using the console.
• Disable the console port. We recommend disabling the console port to prevent unauthorized access to the device, especially when the device is used as customer premises equipment (CPE) and is forwarding sensitive traffic.

**NOTE:** It is not always possible to disable the console port, because console access is important during operations such as software upgrades.

**WARNING:** On SRX SRX300, SRX320, SRX340, and SRX345 devices, if both `set system ports console insecure` and `set chassis routing-engine bios uninterrupt` options are configured, there is no alternative recovery method available incase Junos OS fails to boot and the device might become unusable.

To secure the console port:

1. Do one of the following:
   • Disable the console port. Enter
     
     ```
     [edit system ports console]
     user@host# set disable
     ```
   • Disable root login connections to the console. Enter
     
     ```
     [edit system ports console]
     user@host# set insecure
     ```

   **NOTE:** After configuring the console port as insecure, if a user tries to perform password recovery operation by booting in single-user mode, the device will prompt for the root password. This way, the user will be unable to log in to single-user mode for password recovery unless the root password is known.

   • Log out the console session when the serial cable connected to the console port is unplugged. Enter
NOTE: The `log-out-on-disconnect` statement is not operational on SRX1500, SRX4100, SRX4200, and SRX4600 devices; on these devices, you must manually log out from the console with the `request system logout` command.

2. If you are done configuring the device, enter `commit` from configuration mode.

**Securing Mini-USB Ports**

SRX320, SRX320, SRX340, and SRX345 devices have a mini-USB Type-B port. You can connect your management device to the Mini-USB Type-B console port for CLI management.

You can disable mini-USB ports on the SRX Series devices to block users from connecting a USB mass storage device to the services gateway. When you disable the device, any transactions in progress on the USB device are aborted.

Disable mini-USB ports.

- Use the following command to disable the mini-USB ports.

  ```
  [edit]
  user@host# set chassis usb storage disable
  ```

Enable mini-USB ports.

- Use the following command to enable the mini-USB ports.

  ```
  [edit]
  user@host# delete chassis usb storage disable
  ```

  This step re-enables the disabled mini-USB ports.

Verify the status of the mini-USB.

- Use the following `show` command to verify the status.
user@host> show chassis usb storage

The output displays the current status of USB mass storage device and whether the USB ports are enabled or disabled.

USB Enabled

RELATED DOCUMENTATION

- Console Port Overview
Access Control on Switches

Access Control and Authentication on Switching Devices | 361

Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot | 373

RADIUS Server Configuration for Authentication | 378

802.1X Authentication | 386

MAC RADIUS Authentication | 425

802.1X and RADIUS Accounting | 434

Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch | 440

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

Interfaces Enabled for 802.1X or MAC RADIUS Authentication | 456

Static MAC Bypass of 802.1X and MAC RADIUS Authentication | 477

Captive Portal Authentication | 485

Flexible Authentication Order on EX Series Switches | 505

Central Web Authentication | 510
Access Control and Authentication on Switching Devices

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. Read this topic for more information.

Understanding Authentication on Switches

IN THIS SECTION

- Sample Authentication Topology | 362
- 802.1X Authentication | 364
- MAC RADIUS Authentication | 365
- Captive Portal Authentication | 366
- Static MAC Bypass of Authentication | 366
- Fallback of Authentication Methods | 367
You can control access to your network through a Juniper Networks EX Series Ethernet Switch by using authentication methods such as 802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthenticated devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a Dynamic Host Configuration Protocol (DHCP) server. For captive portal authentication, the switch allows the end devices to acquire an IP address in order to redirect them to a login page for authentication.

This topic covers:

Sample Authentication Topology

Figure 5 on page 363 illustrates a basic deployment topology for authentication on an EX Series switch:

NOTE: For illustration purposes, we have used an EX Series switch, but a QFX5100 switch can be used in the same way.
The topology contains an EX Series access switch connected to the authentication server on port ge-0/0/10. Interface ge-0/0/1 connects to the conference room host. Interface ge-0/0/8 is connected to four desktop PCs through a hub. Interfaces ge-0/0/9 and ge-0/0/2 are connected to IP phones with an integrated hub.
to connect the phone and desktop PC to a single port. Interfaces ge-0/0/19 and ge-0/0/20 are connected to printers.

**802.1X Authentication**

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism for devices seeking to access a LAN. The 802.1X authentication feature on an EX Series switch is based upon the IEEE 802.1X standard *Port-Based Network Access Control*.

The communication protocol between the end device and the switch is Extensible Authentication Protocol over LAN (EAPoL). EAPoL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the switch is RADIUS.

During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic and control traffic can transit the network. Other traffic, such as DHCP traffic and HTTP traffic, is blocked at the data link layer.

**NOTE:** You can configure both the maximum number of times an EAPoL request packet is retransmitted and the timeout period between attempts. For information, see “Configuring 802.1X Interface Settings (CLI Procedure)” on page 390.

An 802.1X authentication configuration for a LAN contains three basic components:

- **Supplicant** (also called end device)—Supplicant is the IEEE term for an end device that requests to join the network. The end device can be responsive or nonresponsive. A responsive end device is 802.1X-enabled and provides authentication credentials using EAP. The credentials required depend on the version of EAP being used—specifically, a username and password for EAP MD5 or a username and client certificates for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected EAP (PEAP).

You can configure a server-reject VLAN to provide limited LAN access for responsive 802.1X-enabled end devices that sent incorrect credentials. A server-reject VLAN can provide a remedial connection, typically only to the Internet, for these devices. See “Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients” on page 415 for additional information.

**NOTE:** If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is dropped.

A nonresponsive end device is one that is not 802.1X-enabled. It can be authenticated through MAC RADIUS authentication.
• **Authenticator port access entity**—The IEEE term for the authenticator. The switch is the authenticator, and it controls access by blocking all traffic to and from end devices until they are authenticated.

• **Authentication server**—The authentication server contains the backend database that makes authentication decisions. It contains credential information for each end device that is authenticated to connect to the network. The authenticator forwards credentials supplied by the end device to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied. The EX Series switches support RADIUS authentication servers.

**NOTE:** You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information about RTGs, see *Understanding Redundant Trunk Links (Legacy RTG Configuration)*.

**MAC RADIUS Authentication**

The 802.1X authentication method only works if the end device is 802.1X-enabled, but many single-purpose network devices such as printers and IP phones do not support the 802.1X protocol. You can configure MAC RADIUS authentication on interfaces that are connected to network devices that do not support 802.1X and for which you want to allow to access the LAN. When an end device that is not 802.1X-enabled is detected on the interface, the switch transmits the MAC address of the device to the authentication server. The server then tries to match the MAC address with a list of MAC addresses in its database. If the MAC address matches an address in the list, the end device is authenticated.

You can configure both 802.1X and MAC RADIUS authentication methods on the interface. In this case, the switch first attempts to authenticate the end device by using 802.1X, and if that method fails, it attempts to authenticate the end device by using MAC RADIUS authentication. If you know that only non-responsive supplicants connect on that interface, you can eliminate the delay that occurs for the switch to determine that the end device is not 802.1X-enabled by configuring the `mac-radius-restrict` option. When this option is configured, the switch does not attempt to authenticate the end device through 802.1X authentication but instead immediately sends a request to the RADIUS server for authentication of the MAC address of the end device. If the MAC address of that end device is configured as a valid MAC address on the RADIUS server, the switch opens LAN access to the end device on the interface to which it is connected.

The `mac-radius-restrict` option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. If you configure `mac-radius-restrict` on an interface, the switch drops all 802.1X packets.

The authentication protocols supported for MAC RADIUS authentication are EAP-MD5, which is the default, Protected EAP (EAP-PEAP), and Password Authentication Protocol (PAP). You can specify the authentication protocol to be used for MAC RADIUS authentication using the `authentication-protocol` statement.
Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) enables you to authenticate users on EX Series switches by redirecting Web browser requests to a login page that requires users to input a valid username and password before they can access the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database by using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos operating system (Junos OS) for EX Series switches provides a template that enables you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time an end device connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. After the device is successfully authenticated, it is allowed access to the network and to continue to the original page requested.

NOTE: If HTTPS is enabled, HTTP requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the end device is returned to the HTTP connection.

If there are end devices that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC addresses to an authentication whitelist.

When a user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Captive portal on switches has the following limitations:

- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user remains idle for more than about 5 minutes and there is no traffic passed, the user must log back in to the captive portal.

Static MAC Bypass of Authentication

You can allow end devices to access the LAN without authentication on a RADIUS server by including their MAC addresses in the static MAC bypass list (also known as the exclusion list).

You might choose to include a device in the bypass list to:

- Allow non-802.1X-enabled devices access to the LAN.
- Eliminate the delay that occurs for the switch to determine that a connected device is a non-802.1X-enabled host.
When you configure static MAC on the switch, the MAC address of the end device is first checked in a local database (a user-configured list of MAC addresses). If a match is found, the end device is successfully authenticated and the interface is opened up for it. No further authentication is done for that end device. If a match is not found and 802.1X authentication is enabled on the switch, the switch attempts to authenticate the end device through the RADIUS server.

For each MAC address, you can also configure the VLAN to which the end device is moved or the interfaces on which the host connects.

CAUTION: When you clear the learned MAC addresses from an interface, using the `clear dot1x interface` command, all MAC addresses are cleared, including those in the static MAC bypass list.

Fallback of Authentication Methods

You can configure 802.1X, MAC RADIUS, and captive portal authentication on a single interface to enable fallback to another method if authentication by one method fails. The authentication methods can be configured in any combination, except that you cannot configure both MAC RADIUS and captive portal on an interface without also configuring 802.1X. By default, an EX Series switch uses the following order of authentication methods:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.

2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.

3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after the other authentication methods configured on the interface have failed.

For an illustration of the default process flow when multiple authentication methods are configured on an interface, see "Understanding Access Control on Switches" on page 368.

You can override the default order for fallback of authentication methods by configuring the `authentication-order` statement to specify that the switch use either 802.1X authentication or MAC RADIUS authentication first. Captive portal must always be last in the order of authentication methods. For more information, see "Configuring Flexible Authentication Order" on page 506.
NOTE: Starting with Junos OS Release 15.1R3, if an interface is configured in multiple-suppliant mode, end devices connecting through the interface can be authenticated using different methods in parallel. Therefore, if an end device on the interface was authenticated after fall back to captive portal, then additional end devices can still be authenticated using 802.1X or MAC RADIUS authentication.

SEE ALSO

- 802.1X for Switches Overview | 387
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring MAC RADIUS Authentication (CLI Procedure) | 426
- Configuring Captive Portal Authentication (CLI Procedure) | 492
- Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure) | 478

**Understanding Access Control on Switches**

You can control access to your network through a switch by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

*Figure 6 on page 369* illustrates the authentication process:
Figure 6: Authentication Process Flow for Switches

SEE ALSO

Understanding Server Fail Fallback and Authentication on Switches | 383
Understanding Guest VLANs for 802.1X on Switches | 407
Understanding Dynamic VLAN Assignment Using RADIUS Attributes | 406
Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Understanding Authentication Session Timeout

Information about authentication sessions—including the associated interfaces and VLANs for each MAC address that is authenticated—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured `mac-table-aging-time` value, the MAC address is removed from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication session table, with the result that the session ends.

When the authentication session ends due to MAC address aging, the host must re-attempt authentication. To limit the downtime resulting from re-authentication, you can control the timeout of authentication sessions in the following ways:

- For 802.1X and MAC RADIUS authentication sessions, disassociate the authentication session table from the Ethernet switching table by using the `no-mac-table-binding` statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.

- For captive portal authentication sessions, configure a keep-alive timer using the `user-keepalive` statement. With this option configured, when the associated MAC address ages out of the Ethernet switching table, the keep-alive timer is started. If traffic is received within the keep-alive timeout period, the timer is deleted. If there is no traffic within the keep-alive timeout period, the session is deleted.

You can also specify timeout values for authentication sessions to end the session before the MAC aging timer expires. After the session times out, the host must re-attempt authentication.

- For 802.1X and MAC RADIUS authentication sessions, the duration of the session before timeout depends on the value of the `reauthentication` statement. If the MAC aging timer expires before the session times out, and the `no-mac-table-binding` statement is not configured, the session is ended, and the host must re-authenticate.

- For captive portal authentication sessions, the duration of the session depends on the value configured for the `session-expiry` statement. If the MAC aging timer expires before the session times out, and the `user-keepalive` statement is not configured, the session is ended, and the host must re-authenticate.

**NOTE:** If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using either the `reauthentication` statement of the `session-expiry` statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message. For information about configuring the authentication server to send an authentication session timeout, see the documentation for your server.
Controlling Authentication Session Timeouts (CLI Procedure)

The expiration of an authentication session can result in downtime because the host must re-attempt authentication. You can limit this downtime by controlling the timeout period for authentication sessions.

An authentication session can end when the MAC address associated with the authenticated host ages out of the Ethernet switching table. When the MAC address is cleared from the Ethernet switching table, the authenticated session for that host ends, and the host must re-attempt authentication.

To prevent the authentication session from ending when the MAC address ages out of the Ethernet switching table:

- For sessions authenticated using 802.1X or MAC RADIUS authentication, you can prevent authentication session timeouts due to MAC address aging by disassociating the authentication session table from the Ethernet switching table using the `no-mac-table-binding` statement:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator no-mac-table-binding;
  ```

- For sessions authenticated using captive portal authentication, you can prevent authentication session timeouts due to MAC address aging by extending the timeout period using the `user-keepalive` statement:

  ```
  [edit]
  user@switch# set services captive-portal interface interface-name user-keepalive minutes;
  ```

You can also configure timeout values for authentication sessions to end an authenticated session before the MAC aging timer expires.

**NOTE:** Configuring the session timeout for an authentication session does not extend the session after the MAC aging timer expires. You must configure either the `no-mac-table-binding` statement for 802.1X and MAC RADIUS authentication, or the `user-keepalive` statement for captive portal authentication, to prevent session timeout due to MAC aging.
For 802.1X and MAC RADIUS authentication sessions, configure the timeout value using the `reauthentication` statement.

- To configure the timeout value on a single interface:
  
  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name reauthentication seconds;
  ```

- To configure the timeout value on all interfaces:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface all reauthentication seconds;
  ```

For captive portal authentication sessions, configure the timeout value using the `session-expiry` statement.

- To configure the timeout value on a single interface:

  ```
  [edit]
  user@switch# set services captive-portal interface interface-name session-expiry minutes;
  ```

- To configure the timeout value on all interfaces:

  ```
  [edit]
  user@switch# set services captive-portal interface all session-expiry minutes;
  ```

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured using the `reauthentication` statement or the `session-expiry` statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

SEE ALSO

* Configuring MAC Table Aging on Switches

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440

RELATED DOCUMENTATION

* 802.1X Authentication | 386
Preventing Unauthorized Access to EX Series Switches Using Unattended Mode for U-Boot

IN THIS SECTION

- Understanding Unattended Mode for U-Boot on EX Series Switches | 373
- Using Unattended Mode for U-Boot to Prevent Unauthorized Access | 375

Junos OS allows you to configure an unattended mode for U-Boot to prevent unauthorized access to the switch during the boot process. When you configure unattended mode, a user can access the CLI during the boot process by supplying the boot-loader password. This prevents unauthorized access during boot process. Read this topic for more information.

Understanding Unattended Mode for U-Boot on EX Series Switches

Unattended mode for U-Boot can be configured to prevent unauthorized access to the switch that can occur during the boot process. After the CPU has been reset, there are several known methods of accessing the system before the JUNOS OS login prompt appears that do not require the user to enter authorization credentials. By gaining unauthorized access, the user can view, modify, or corrupt the switch configuration, or make the switch unavailable on the network.

When unattended mode is configured, the user can access the CLI during the boot process only by pressing <Ctrl+c> and entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch. Entering the correct boot-loader password will place the user in the U-Boot CLI. If the password is incorrect, or if no password is entered within one minute, access to the U-Boot CLI is blocked and the boot process continues automatically.

Access to the bootstrap loader command prompt (loader>) is blocked in unattended mode, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.
NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see Reverting to the Default Factory Configuration for the EX Series Switch.

If unattended mode is not configured, but a boot-loader password has been configured, the user must enter the correct password to access the U-Boot CLI. If a boot-loader password has not been configured, the user can access the U-Boot CLI without entering a password. In either case, the user can access the bootstrap loader command prompt, which enables root password recovery by using single-user mode as well as booting from a USB flash drive.

Unattended mode is not enabled by default. When configured, unattended mode is turned on and will block unauthorized access to the switch. Table 22 on page 374 summarizes the behaviors for U-Boot mode.

### Table 22: Unattended Mode Behavior

<table>
<thead>
<tr>
<th>Unattended Mode</th>
<th>Boot-loader password</th>
<th>Behavior</th>
</tr>
</thead>
</table>
| **On**          | Set                  | - Access to U-Boot CLI is allowed only after entering correct password.  
                  |                      | - Access to loader command prompt is blocked.  
                  |                      | - Booting from USB is blocked.  
                  |                      | - Root password recovery by using single-user mode is blocked. |
| **On**          | Not Set              | - Access to U-Boot CLI is blocked.  
                  |                      | - Access to loader command prompt is blocked.  
                  |                      | - Booting from USB is blocked.  
                  |                      | - Root password recovery by using single-user mode is blocked. |
| **Off**         | Set                  | - Access to U-Boot CLI is allowed only after entering correct password.  
                  |                      | - Access to loader command prompt is allowed.  
                  |                      | - Booting from USB is allowed.  
                  |                      | - Root password recovery by using single-user mode is allowed. |
| **Off**         | Not Set              | - Access to U-Boot CLI is allowed.  
                  |                      | - Access to loader command prompt is allowed.  
                  |                      | - Booting from USB is allowed.  
                  |                      | - Root password recovery by using single-user mode is allowed. |

SEE ALSO
Using Unattended Mode for U-Boot to Prevent Unauthorized Access

Unattended mode for U-Boot can be used to prevent unauthorized access to the switch that can occur during the boot process. When unattended mode is configured, the user can access the CLI during the boot process only by entering the correct password, which is known as the boot-loader password. The boot-loader password must have been previously configured on the switch.

When unattended mode is configured, access to the bootstrap loader command prompt (loader>) is blocked, which prevents the use of the following recovery mechanisms: root password recovery by using single-user mode, and booting the switch by using a software package stored on a USB flash drive.

WARNING: On EX2200 switches, if both the root and unattended mode password are lost while the switch is in unattended mode, there is no alternative recovery method available. The switch must be returned to Juniper Networks. For more information, see Returning an EX2200 Switch or Component for Repair or Replacement.

To use unattended mode, follow the following procedures:
Configuring the Boot Loader Password

To configure the boot loader password, you can use either a plain-text password that the system encrypts for you, or a password that has already been encrypted. If you use a plain-text password, Junos OS displays the password as an encrypted string so that users viewing the configuration cannot see it. As you enter the password in plain text, Junos OS encrypts it immediately. You do not have to configure Junos OS to encrypt the password. Plain-text passwords are hidden and marked as ## SECRET-DATA in the configuration.

To configure the boot-loader password:

1. Enter either a plain-text password or an encrypted password by using the set system boot-loader authentication command.

   • To enter a plain-text password, use the plain-text-password option, and re-enter the password when prompted:

     ```
     [edit]
     root@# set system boot-loader-authentication plain-text-password
     New Password: type password here
     Retype new password: retype password here
     ```

   • To enter a password that is already encrypted, use the encrypted-password option:

     ```
     [edit]
     root@# set system boot-loader-authentication encrypted-password password
     ```

2. Commit the changes.

   ```
   [edit]
   root@# commit
   ```

3. To view the encrypted password entries, use the configuration mode show command. For example:

   ```
   [edit]
   root@# show system boot-loader-authentication
   encrypted-password "$ABC123"; ## SECRET-DATA
   ```
Configuring Unattended Mode for U-Boot

Before enabling unattended mode for U-Boot, you must download and install the jloader firmware package /volume/build/junos/13.2/service/13.2X51-D20.2/ship/jloader-ex-2200-13.2X51-D20.2-signed.tgz, as described in TSB16425.

Unattended mode for U-Boot is not enabled by default. Use the following procedure to configure unattended mode:

1. Configure unattended mode.

   [edit]
   root@# set system unattended-boot

2. Commit the changes.

   [edit]
   root@# commit

Accessing the U-Boot CLI

When unattended mode for U-Boot is configured and the boot-loader password has been set, you can access the U-Boot CLI during the boot process by pressing <Ctrl+c> and entering the password at the prompt:

Press Ctrl-C in next 1 seconds to enter u-boot prompt...
Enter password:
password correct...
=>

The correct password must be entered within one minute after the prompt appears. If the password is not entered within one minute, or if the password is incorrect or has not been configured, access to the U-Boot CLI will be blocked, and the boot process will continue. For more information about unattended mode behavior, see “Understanding Unattended Mode for U-Boot on EX Series Switches” on page 373.

SEE ALSO

<table>
<thead>
<tr>
<th>unattended-boot</th>
<th>2381</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot-loader-authentication</td>
<td>1538</td>
</tr>
</tbody>
</table>
Juniper Networks Ethernet Switches use 802.1X, MAC RADIUS, or captive portal authentication to provide access control to the devices or users. When 802.1X, MAC RADIUS, or captive portal authentications are configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you want to connect. Read this topic for more information.
IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure a RADIUS server on the switch:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the switch must match the secret password on the server:

   ```
   [edit access]
   user@switch# set radius-server server-address port 1812 secret password
   ```

   **NOTE:** Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify the IP address, the RADIUS server uses the address of the interface that sends the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch:

   ```
   [edit access]
   user@switch# set access radius-server source-address source-address
   ```

3. Configure the authentication order, making radius the first method of authentication:

   ```
   [edit access]
   user@switch# set profile profile-name authentication-order (Access Profile) radius
   ```

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers.
[edit access profile profile-name]
user@switch# set radius authentication-server server-address server-address

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

[edit]
user@switch# set protocols dot1x authenticator authentication-profile-name access-profile-name

6. Configure the IP address of the switch in the list of clients on the RADIUS server. For information about configuring the RADIUS server, consult the documentation for your server.

SEE ALSO

- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring MAC RADIUS Authentication (CLI Procedure) | 426
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438

## Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

Junos OS for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433, *Microsoft PPP CHAP Extensions*, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:
Configured RADIUS server authentication. Configure users on the authentication server and set the first-tried option in the authentication order to radius. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

SEE ALSO

Managing Users (J-Web Procedure)

For more about configuring user access, see the Junos OS Access Privilege Configuration Guide.

**Configuring MS-CHAPv2 for Password-Change Support**

You can configure the Microsoft implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the router or switch to support changing of passwords. This feature provides users accessing a router or switch the option of changing the password when the password expires, is reset, or is configured to be changed at next logon.

Before you configure MS-CHAPv2 for password-change support, ensure that you have done the following:

- Configured RADIUS server authentication parameters.
- Set the first tried option in the authentication order to RADIUS server.

To configure MS-CHAP-v2, include the following statements at the [edit system radius-options] hierarchy level:

```
[edit system radius-options]
password-protocol mschap-v2;
```

The following example shows statements for configuring the MS-CHAPv2 password protocol, password authentication order, and user accounts:

```
[edit]
system {
```
authentication-order [ radius password ];
radius-server {
    192.168.69.149 secret "$9$G-j.5Qz6tpBk.1hrlXxUjiq5Qn/C"; ## SECRET-DATA
}
radius-options {
    password-protocol mschap-v2;
}
login {
    user bob {
        class operator;
    }
}

SEE ALSO

Configuring Access Profiles for L2TP or PPP Parameters
Understanding Server Fail Fallback and Authentication on Switches

Juniper Networks Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication is configured on the switch, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

Server fail fallback enables you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device’s first attempt at authentication through the RADIUS server.

Server fail fallback enables you to specify one of four actions to be taken for end devices awaiting authentication when the server is timed out. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch. The configured VLAN name overrides any attributes sent by the server.

- **Permit** authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- **Deny** authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- **Move** the end device to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server. (The VLAN must already exist on the switch.)
- **Sustain** authenticated end devices that already have LAN access and **deny** unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

SEE ALSO

- **802.1X for Switches Overview**  | 387
- **Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch**  | 408
- **Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch**  | 440
- **Configuring 802.1X Interface Settings (CLI Procedure)**  | 390
Configuring RADIUS Server Fail Fallback (CLI Procedure)

You can configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. If this happens, because it is the authentication server that grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN, and normal authentication cannot be completed.

You can configure the server fail fallback feature to specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN.

You can also configure the server reject fallback feature for end devices that receive a RADIUS access-reject message from the authentication server. The server reject fallback feature provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4. To configure server fail fallback actions for VoIP clients sending voice traffic, use the server-fail-voip statement. For all data traffic, use the server-fail statement. The switch determines the fallback method to use based on the type of traffic sent by the client. Untagged data frames are subject to the action configured with server-fail, even if they are sent by a VoIP client. Tagged VoIP VLAN frames are subject to the action configured with server-fail-voip. If server-fail-voip is not configured, the voice traffic is dropped.

NOTE: Server reject fallback is not supported for VoIP VLAN tagged traffic. If a VoIP client starts authentication by sending untagged data traffic to a VLAN while server reject fallback is in effect, the VoIP client is allowed to access the fallback VLAN. If the same client subsequently sends tagged voice traffic, the voice traffic is dropped.

If a VoIP client starts authentication by sending tagged voice traffic while server reject fallback is in effect, the VoIP client is denied access to the fallback VLAN.
You can use the following procedure to configure server fail actions for data clients. To configure server fail fallback for VoIP clients sending voice traffic, use the `server-fail-voip` statement in place of the `server-fail` statement.

To configure server fail fallback actions:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail permit
  ```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been denied access by the RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail deny
  ```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs:

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail vlan-name
  ```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new end devices are denied access):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-fail use-cache
  ```

You can configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a server-reject VLAN, a specified VLAN already configured on the switch.

To configure a server reject fallback VLAN:

- ```
  [edit protocols dot1x authenticator]
  user@switch# set interface interface-name server-reject-vlan vlan-sf
  ```

SEE ALSO

- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 408
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1X53-D40</td>
<td>Server fail fallback is supported for voice traffic starting in Release 14.1X53-D40 and Release 15.1R4.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- Access Control and Authentication on Switching Devices | 361
- 802.1X Authentication | 386
- 802.1X and RADIUS Accounting | 434
- MAC RADIUS Authentication | 425

802.1X Authentication

IN THIS SECTION

- 802.1X for Switches Overview | 387
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Understanding RADIUS-Initiated Changes to an Authorized User Session | 392
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Understanding Dynamic Filters Based on RADIUS Attributes | 405
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes | 406
- Understanding Guest VLANs for 802.1X on Switches | 407
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 408
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients | 415
- Monitoring 802.1X Authentication | 420
IEEE 802.1X standard for port-based network access control and protects Ethernet LANs from unauthorized user access. It blocks all traffic to and from a supplicant (client) at the interface until the supplicant’s credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant. Read this topic for more information.

### 802.1X for Switches Overview

#### How 802.1X Authentication Works

802.1X authentication works by using an authenticator port access entity (the switch) to block ingress traffic from a supplicant (end device) at the port until the supplicant's credentials are presented and match on the authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in single supplicant mode, single-secure supplicant mode, or multiple supplicant mode:

- **single supplicant**—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively piggyback on the first end device’s authentication.

- **single-secure supplicant**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first device logs out.

- **multiple supplicant**—Allows multiple end devices to connect to the port. Each end device is authenticated individually.

Network access can be further defined by using VLANs and firewall filters, both of which act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.

- Whether or not MAC RADIUS authentication is configured on the switch interfaces to which the hosts are connected.
• Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See "Configuring RADIUS Server Fail Fallback (CLI Procedure)" on page 384.

802.1X Features Overview

The following 802.1X features are supported on Juniper Networks Ethernet Switches:

• Guest VLAN—Provides limited access to a LAN, typically only to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication is not configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access only to the Internet and to other guests’ end devices.

• Server-reject VLAN—Provides limited access to a LAN, typically only to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

• Server-fail VLAN—Provides limited access to a LAN, typically only to the Internet, for 802.1X end devices during a RADIUS server timeout.

• Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.

• Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).

• Dynamic changes to a user session—Enables the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.

• VoIP VLAN—Supports IP telephones. The implementation of a voice VLAN on an IP telephone is vendor-specific. If the phone is 802.1X-enabled, it is authenticated as any other supplicant is. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (provided that the interface is configured in single supplicant mode and not in single-secure supplicant mode).

NOTE: Configuring a VoIP VLAN on private VLAN (PVLAN) interfaces is not supported.

• RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

• RADIUS server attributes for 802.1X—The Juniper-Switching-Filter is a vendor-specific attribute (VSA) that can be configured on the RADIUS server to further define a supplicant’s access during the 802.1X authentication process. Centrally configuring attributes on the authentication server obviates the need
to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant might connect to the LAN. This feature is based on RLI 4583, AAA RADIUS BRAS VSA Support.

The following features are supported to authenticate devices that are not 802.1X-enabled:

- **Static MAC bypass**—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.

- **MAC RADIUS authentication**—Provides a means to permit hosts that are not 802.1X-enabled to access the LAN. MAC-RADIUS simulates the supplicant functionality of the client device, using the MAC address of the client as username and password.

### 802.1X Authentication on Trunk Ports

Starting in Junos OS Release 18.3R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device. An AP or switch connected to the NAS will support multiple VLANs, so must connect to a trunk port. Enabling 802.1X authentication on the trunk interface protects the NAS from a security breach in which an attacker might disconnect the AP and connect a laptop to get free access to network for all the configured VLANs.

Please note the following caveats when configuring 802.1X authentication on trunk interfaces.

- Only single and single-secure supplicant modes are supported on trunk interfaces.

- You must configure 802.1X authentication locally on the trunk interface. If you configure 802.1X authentication globally using the `set protocol dot1x interface all` command, the configuration is not applied to the trunk interface.

- Dynamic VLANS are not supported on trunk interfaces.

- Guest VLAN and server-reject VLAN are not supported on trunk interfaces.

- Server fail fallback for VoIP clients is not supported on trunk interfaces (`server-fail-voip`).

- Authentication on trunk port is not supported using captive portal.

- Authentication on trunk port is not supported on aggregated interfaces.

- Configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANS) is not supported on trunk ports.

**SEE ALSO**

| Understanding Authentication on Switches | 361 |
Configuring 802.1X Interface Settings (CLI Procedure)

IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant’s credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:
- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See "Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)" on page 478.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See "Specifying RADIUS Server Connections on Switches (CLI Procedure)" on page 379.

To configure 802.1X on an interface:

1. Configure the supplicant mode as single (authenticates the first supplicant), single-secure (authenticates only one supplicant), or multiple (authenticates multiple supplicants):

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface interface-name supplicant multiple
   ```

   NOTE: Multiple supplicant mode is not supported on trunk interfaces.

2. Enable reauthentication and specify the reauthentication interval:

   ```
   [edit protocols dot1x]
   ```
user@switch# set authenticator interface interface-name reauthentication interval seconds

3. Configure the interface timeout value for the response from the supplicant:

[edit protocols dot1x]
user@switch# set authenticator interface interface-name supplicant-timeout seconds

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

[edit protocols dot1x]
user@switch# set authenticator interface interface-name server-timeout seconds

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

[edit protocols dot1x]
user@switch# set authenticator interface interface-name transmit-period seconds

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

[edit protocols dot1x]
user@switch# set authenticator interface interface-name maximum-requests number

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

[edit protocols dot1x]
user@switch# set authenticator interface interface-name retries (802.1X) number

NOTE: This setting specifies the number of attempts before the switch puts the interface in a HELD state.

SEE ALSO

- Configuring 802.1X Authentication (J-Web Procedure)
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Configuring LLDP (CLI Procedure) | 654
Understanding RADIUS-Initiated Changes to an Authorized User Session

IN THIS SECTION
- Disconnect Messages | 392
- Change of Authorization Messages | 393
- CoA Request Port Bounce | 393
- Error-Cause Codes | 394

When using an authentication service that is based on a client/server RADIUS model, requests are typically initiated by the client and sent to the RADIUS server. There are instances in which a request might be initiated by the server and sent to the client in order to dynamically modify an authenticated user session already in progress. The client that receives and processes the messages is the switch, which acts as the network access server, or NAS. The server can send the switch a Disconnect message requesting to terminate a session, or a Change of Authorization (CoA) message requesting to modify the session authorization attributes.

The switch listens for unsolicited RADIUS requests on UPD port 3799, and accepts requests only from a trusted source. Authorization to send a Disconnect or CoA request is determined based on the source address and the corresponding shared secret, which must be configured on the switch as well as on the RADIUS server. For more information about configuring the source address and shared secret on the switch, see “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.

Disconnect Messages

The RADIUS server sends a Disconnect-Request message to the switch in order to terminate a user session and discard all associated session context. The switch responds to a Disconnect-Request packet with a Disconnect-ACK message if the request is successful, that is, all associated session context is discarded and the user session is no longer connected, or with a Disconnect-NAK packet if the request fails, that is, the authenticator is unable to disconnect the session and discard all associated session context.

In Disconnect-Request messages, RADIUS attributes are used to uniquely identify the switch (NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match at least one session for the request to be successful; otherwise, the switch responds with a Disconnect-NAK message. A Disconnect-Request message can contain only NAS
and session identification attributes; if any other attributes are included, the switch responds with a Disconnect-NAK message.

**Change of Authorization Messages**

Change of Authorization (CoA) messages contain information for dynamically modifying the authorization attributes for a user session to change the authorization level. This occurs as part of a two-step authentication process, in which the endpoint is first authenticated using MAC RADIUS authentication, and is then profiled based on the type of device. The CoA message is used to apply an enforcement policy that is appropriate for the device, typically by changing the data filters or the VLAN.

The switch responds to a CoA message with a CoA-ACK message if the authorization change is successful, or a with CoA-NAK message if the change is unsuccessful. If one or more authorization changes specified in a CoA-Request message cannot be carried out, the switch responds with a CoA-NAK message.

In CoA-Request messages, RADIUS attributes are used to uniquely identify the switch (acting as the NAS) and the user session. The combination of NAS identification attributes and session identification attributes included in the message must match the identification attributes of at least one session for the request to be successful; otherwise, the switch responds with a CoA-NAK message.

CoA-Request packets also include the session authorization attributes that will be modified if the request is accepted. The supported session authorization attributes are listed below. The CoA message can contain any or all of these attributes. If any attribute is not included as part of the CoA-Request message, the NAS assumes that the value for that attribute is to remain unchanged.

- Filter-ID
- Tunnel-Private-Group-ID
- Juniper-Switching-Filter
- Juniper-VoIP-VLAN
- Session-Timeout

**CoA Request Port Bounce**

When a CoA message is used to change the VLAN for an authenticated host, end devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.

The command to bounce the port is sent from the RADIUS server using a Juniper Networks vendor-specific attribute (VSA). The port is bounced if the following VSA attribute-value pair is received in the CoA message from the RADIUS server:
• Juniper-AV-Pair = “Port-Bounce”

To enable the port bounce feature, you must update the Junos dictionary file (juniper.dct) on the RADIUS server with the Juniper-AV-Pair VSA. Locate the dictionary file and add the following text to the file:

```
ATTRIBUTE Juniper-AV-Pair  Juniper-VSA(52, string) r
```

For more information about adding the VSA, consult the FreeRADIUS documentation.

You can disable the feature by configuring the `ignore-port-bounce` statement at the `[edit protocols dot1x authenticator interface interface-name mac-radius]` hierarchy level.

**Error-Cause Codes**

When a disconnect or CoA operation is unsuccessful, an Error-Cause attribute (RADIUS attribute 101) can be included in the response message sent by the NAS to the server to provide detail about the cause of the problem. If the detected error does not map to one of the supported Error-Cause attribute values, the router sends the message without an error-cause attribute. See Table 23 on page 394 for descriptions of error-cause codes that can be included in response messages sent from the NAS.

**Table 23: Error-Cause Codes (RADIUS Attribute 101)**

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual session context removed</td>
<td>Sent in response to a Disconnect-Request message if one or more user sessions are no longer active, but residual session context was found and successfully removed. This code is sent only within a Disconnect-ACK message.</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported attribute</td>
<td>The request contains an attribute that is not supported (for example, a third-party attribute).</td>
</tr>
<tr>
<td>402</td>
<td>Missing attribute</td>
<td>A critical attribute (for example, the session identification attribute) is missing from a request.</td>
</tr>
<tr>
<td>403</td>
<td>NAS identification mismatch</td>
<td>Request contains one or more NAS identification attributes that do not match the identity of the NAS receiving the request.</td>
</tr>
<tr>
<td>404</td>
<td>Invalid request</td>
<td>Some other aspect of the request is invalid—for example, if one or more attributes are not formatted properly.</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported service</td>
<td>The Service-Type attribute included with the request contains an invalid or unsupported value.</td>
</tr>
</tbody>
</table>
Table 23: Error-Cause Codes (RADIUS Attribute 101) (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>406</td>
<td>Unsupported extension</td>
<td>The entity receiving the request (either an NAS or a RADIUS proxy) does not support RADIUS-initiated requests.</td>
</tr>
<tr>
<td>407</td>
<td>Invalid attribute value</td>
<td>The request contains an attribute with an unsupported value.</td>
</tr>
<tr>
<td>501</td>
<td>Administratively prohibited</td>
<td>The NAS is configured to prohibit honoring of Disconnect-Request or CoA-Request messages for the specified session.</td>
</tr>
<tr>
<td>503</td>
<td>Session context not found</td>
<td>The session context identified in the request does not exist on the NAS.</td>
</tr>
<tr>
<td>504</td>
<td>Session context not removable</td>
<td>The subscriber identified by attributes in the request is owned by a component that is not supported. This code is sent only within a Disconnect-NAK message.</td>
</tr>
<tr>
<td>506</td>
<td>Resources unavailable</td>
<td>A request could not be honored because of lack of available NAS resources (such as memory).</td>
</tr>
<tr>
<td>507</td>
<td>Request initiated</td>
<td>The CoA-Request message includes a Service-Type attribute with a value of Authorize Only.</td>
</tr>
<tr>
<td>508</td>
<td>Multiple session selection unsupported</td>
<td>The session identification attributes included in the request match multiple sessions, but the NAS does not support requests that apply to multiple sessions.</td>
</tr>
</tbody>
</table>

Filtering 802.1X Supplicants by Using RADIUS Server Attributes

There are two ways to configure the a RADIUS server with port firewall filters (Layer 2 firewall filters):

- Include one or more filter terms in the Juniper-Switching-Filter attribute. The Juniper-Switching-Filter attribute is a vendor-specific attribute (VSA) listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server. Use this VSA to configure simple filter conditions for 802.1X authenticated users. Nothing needs to be configured on the switch; all of the configuration is on the RADIUS server.

- Configure a local firewall filter on each switch and apply that firewall filter to users authenticated through the RADIUS server. Use this method for more complex filters. The firewall filter must be configured on each switch.
NOTE: If the firewall filter configuration is modified after users are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter configuration changes to take effect.

This topic includes the following tasks:

1. Configuring Firewall Filters on the RADIUS Server | 396
2. Applying a Locally Configured Firewall Filter from the RADIUS Server | 399

Configuring Firewall Filters on the RADIUS Server

You can configure simple filter conditions by using the Juniper-Switching-Filter attribute in the Juniper dictionary on the RADIUS server. These filters are sent to a switch whenever a new user is authenticated successfully. The filters are created and applied on all EX Series switches that authenticate users through that RADIUS server without the need for you to configure anything on each individual switch.

NOTE: This procedure describes using FreeRADIUS software to configure the Juniper-Switching-Filter VSA. For specific information about configuring your server, consult the AAA documentation included with your server.

To configure the Juniper-Switching-Filter attribute, enter one or more filter terms by using the CLI for the RADIUS server. Each filter term consists of match conditions with a corresponding action. Enter the filter terms enclosed within quotation marks (“ “) by using the following syntax:

```
Juniper-Switching-Filter = "match <destination-mac mac-address> <source-vlan vlan-name> <source-dot1q-tag tag> <destination-ip ip-address> <ip-protocol protocol-id> <source-port port> <destination-port port> action (allow | deny) <forwarding-class class-of-service> <loss-priority (low | medium | high)>"
```

More than one match condition can be included in a filter term. When multiple conditions are specified in a filter term, they must all be fulfilled for the packet to match the filter term. For example, the following filter term requires a packet to match both the destination IP address and the destination MAC address to meet the term criteria:

```
Juniper-Switching-Filter = "match destination-ip 10.10.10.8 destination-mac 00:00:00:01:02:03 action allow"
```

Multiple filter terms should be separated with commas—for example:
Juniper-Switching-Filter = "match destination-mac 00:00:01:02:03 action allow, match destination-port 80
destination-mac 00:aa:bb:cc:dd:ee action allow"

See "Juniper-Switching-Filter VSA Match Conditions and Actions" on page 251 for definitions of match
conditions and actions.

NOTE: On EX9200 switches, and in a Junos Fusion Enterprise with EX9200 as the aggregate
device, the dynamic firewall filter is strictly applied for all IP packets. If the filter is configured to
allow only a specific destination IP address, packets with other IP addresses as the destination IP
will be dropped per the filter rules. This includes any IP protocol packets, such as DHCP, IGMP and
ARP packets.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the filtering attribute
   Juniper-Switching-Filter (attribute ID 48):

   [root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper

   # dictionary.juniper
   #
   #
   # VENDOR          Juniper                         2636
   BEGIN-VENDOR    Juniper
   ATTRIBUTE       Juniper-Local-User-Name                 1       string
   ATTRIBUTE       Juniper-Allow-Commands                  2       string
   ATTRIBUTE       Juniper-Deny-Commands                   3       string
   ATTRIBUTE       Juniper-Allow-Configuration             4       string
   ATTRIBUTE       Juniper-Deny-Configuration              5       string
   ATTRIBUTE       Juniper-Switching-Filter                48      string
   <-

   2. Enter the match conditions and actions. For example:

      • To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is 10):

        [root@freeradius]#
        cd /usr/local/etc/raddb
        vi users

        For each relevant user, add the Juniper-Switching-Filter attribute:
Juniper-Switching-Filter = "Match Source-dot1q-tag 10 Action deny"

- To deny access based on a destination IP address:

  [root@freeradius]# cd /usr/local/etc/raddb
  vi users

  For each relevant user, add the **Juniper-Switching-Filter** attribute:

  Juniper-Switching-Filter = "Match Destination-ip 192.168.1.0/31 Action deny"

- To set the packet loss priority (PLP) to **high** based on a destination MAC address and the IP protocol:

  [root@freeradius]# cd /usr/local/etc/raddb
  vi users

  For each relevant user, add the **Juniper-Switching-Filter** attribute:

  Juniper-Switching-Filter = "Match Destination-mac 00:04:0f:fd:ac:fe, Ip-protocol 2, forwarding-class high, Action loss-priority high"

**NOTE:** For the **forwarding-class** option to be applied, the forwarding class must be configured on the switch and the packet loss priority specified. If it is not configured on the switch, this option is ignored. You must specify both the forwarding class and the packet loss priority.

3. Stop and restart the RADIUS process to activate the configuration.
Applying a Locally Configured Firewall Filter from the RADIUS Server

You can apply a port firewall filter (Layer 2 firewall filter) to user policies centrally from the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests authentication, reducing the need to configure the same firewall filter on multiple switches. Use this method when the firewall filter contains a large number of conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

For more information about firewall filters, see *Firewall Filters for EX Series Switches Overview*.

To apply a port firewall filter centrally from the RADIUS server:

**NOTE:** If port firewall filters are also configured locally for the interface, then the firewall filters configured by using VSAs take precedence if they conflict with the locally configured port firewall filters. If there is no conflict, they are merged.

1. Create the firewall filter on the local switch. See *Configuring Firewall Filters (CLI Procedure)* for more information on configuring a port firewall filter.

2. On the RADIUS server, open the `users` file to display the local user profiles of the end devices to which you want to apply the filter:

   ```
   [root@freeradius]#
   cat /usr/local/etc/raddb/users
   ```

3. Apply the filter to each user profile by adding the Filter-ID attribute with the filter name as the attribute value:

   ```
   Filter-Id = filter-name
   ```

   For example, the user profile below for `supplicant1` includes the Filter-ID attribute with the filter name `filter1`:

   ```
   [root@freeradius]# cat /usr/local/etc/raddb/users
   ```

   ```
   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-Id = "1005",
   Filter-Id = "filter1"
   ```
NOTE: Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to the switch on the same interface by configuring a single filter with policies for each of those users.

4. Stop and restart the RADIUS process to activate the configuration.

SEE ALSO

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch | 456

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch

IN THIS SECTION

- Requirements | 401
- Overview and Topology | 401
- Configuration | 403
- Verification | 404

802.1X is the IEEE standard for port-based network access control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an EX Series switch, and configure it for 802.1X:
Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
  
  NOTE: For more about ELS, see Using the Enhanced Layer 2 Software CLI.

- Configured users on the RADIUS authentication server.

Overview and Topology

The EX Series switch acts as an authenticator PAE. It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 7 on page 402 shows one EX4200 switch that is connected to the devices listed in Table 24 on page 403.
Figure 7: Topology for Configuration

- Authentication Server
  - RADIUS Server
  - User 1, Password 1
  - User 2, Password 2
  - User n, Password n

- IP Network
- ge-0/0/10

- Conference room host
- ge-0/0/1

- Authenticator Port Access Entity
  - ge-0/0/9

- HUB
- ge-0/0/6

- PC
- ge-0/0/8

- Supplicant (Client)
- ge-0/0/2

- IP Telephone
- ge-0/0/19

- Printer
  - Mac Address: 00:04:ae:ce:23:5f

- Printer
  - Mac Address: 00:04:0f:fd:5e

- PC
- ge-0/0/10
Table 24: Components of the Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, connect the RADIUS server to access port ge-0/0/10 on the EX4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the Junos OS System Basics Configuration Guide.

Configuration

CLI Quick Configuration
To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]
```

Step-by-Step Procedure
To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:
2. Configure the authentication order, making `radius` the first method of authentication:

```
[edit]
user@switch# set access radius-server 10.0.0.100 secret juniper
user@switch# set access radius-server 10.0.0.200 secret juniper
```

3. Configure a list of server IP addresses to be tried in sequential order to authenticate the supplicant:

```
[edit]
user@switch# set access profile profile1 authentication-order radius
```

Results

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
  10.0.0.100
    port 1812;
    secret "$ABC123"; ## SECRET-DATA
}
}
profile profile1{
  authentication-order radius;
  radius {
    authentication-server 10.0.0.100 10.0.0.200;
  }
}
}
```

Verification

**IN THIS SECTION**

- Verify That the Switch and RADIUS Server Are Properly Connected | 405

To confirm that the configuration is working properly, perform these tasks:
Verify That the Switch and RADIUS Server Are Properly Connected

Purpose
Verify that the RADIUS server is connected to the switch on the specified port.

Action
Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

Meaning
ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether the server is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

SEE ALSO
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438

Understanding Dynamic Filters Based on RADIUS Attributes

You can use RADIUS server attributes to implement port firewall filters on a RADIUS authentication server. These filters can be dynamically applied to supplicants that request authentication through that server. RADIUS server attributes are clear-text fields encapsulated in Access-Accept messages sent from the authentication server to the switch when a supplicant connected to the switch is successfully authenticated. The switch, acting as the authenticator, uses the information in the RADIUS attributes to apply the related filters to the supplicant. Dynamic filters can be applied to multiple ports on the same switch, or to multiple switches that use the same authentication server, providing centralized access control for the network.
You can define firewall filters directly on the RADIUS server by using the Juniper-Switching-Filter attribute, which is a RADIUS attribute specific to Juniper Networks, also known as a vendor-specific attribute (VSA). VSAs are described in RFC 2138, Remote Authentication Dial In User Service (RADIUS). The Juniper-Switching-Filter VSA is listed under attribute ID number 48 in the Juniper dictionary on the RADIUS server, with the vendor ID set to the Juniper Networks ID number 2636. Using this attribute, you define filters on the authentication server, which are applied on all switches that authenticate supplicants through that server. This method eliminates the need to configure the same filters on multiple switches.

Alternatively, you can apply a port firewall filter to multiple ports on the same switch by using the Filter-ID attribute, which is RADIUS attribute ID number 11. To use the Filter-ID attribute, you must first configure a filter on the switch, and then add the filter name to user policies on the RADIUS server as the value of the Filter-ID attribute. When a supplicant defined in one of those policies is authenticated by the RADIUS server, the filter is applied to the switch port that has been authenticated for the supplicant. Use this method when the firewall filter has complex conditions, or if you want to use different conditions for the same filter on different switches. The filter named in the Filter-ID attribute must be configured locally on the switch at the edit firewall family ethernet-switching filter hierarchy level.

VSAs are supported only for 802.1X single supplicant configurations and multiple supplicant configurations.

SEE ALSO

| Understanding Authentication on Switches | 361 |
| Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch | 456 |
| Configuring Firewall Filters (CLI Procedure) |
| Juniper-Switching-Filter VSA Match Conditions and Actions | 251 |

### Understanding Dynamic VLAN Assignment Using RADIUS Attributes

VLANs can be dynamically assigned by a RADIUS server to supplicants requesting 802.1X authentication through that server. You configure the VLAN on the RADIUS server using RADIUS server attributes, which are clear-text fields encapsulated in messages sent from the authentication server to the switch when a supplicant connected to the switch requests authentication. The switch, acting as the authenticator, uses the information in the RADIUS attributes to assign the VLAN to the supplicant. Based on the results of the authentication, a supplicant that began authentication in one VLAN might be assigned to another VLAN.

Successful authentication requires that the VLAN ID or VLAN name is configured on the switch acting as 802.1X authenticator, and that it matches the VLAN ID or VLAN name sent by the RADIUS server during authentication.
authentication. If neither exists, the end device is not authenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

The RADIUS server attributes used for dynamic VLAN assignment described in RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*.

- **Tunnel-Type**—Defined as RADIUS attribute type 64. The value should be set to **VLAN**.
- **Tunnel-Medium-Type**—Defined as RADIUS attribute type 65. The value should be set to **IEEE-802**.
- **Tunnel-Private-Group-ID**—Defined as RADIUS attribute type 81. The value should be set to the VLAN ID or the VLAN name.

For more information about configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

**SEE ALSO**

- Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 427
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

**Understanding Guest VLANs for 802.1X on Switches**

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for corporate guests. Guest VLAN is used as a fallback when:

- The supplicant is not 802.1X-enabled and does not respond to EAP messages.
- MAC RADIUS authentication has not been configured on the switch interfaces to which the supplicant is connected.
- Captive portal has not been configured on the switch interfaces to which the supplicant is connected.

A guest VLAN is not used for supplicants that send incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.
Server fail fallback enables you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable.

You use 802.1X to control network access. Only users and devices (supplicants) providing credentials that have been verified against a user database are allowed access to the network. You use a RADIUS server as the user database.

This example describes how to configure an interface to move a supplicant to a VLAN in the event of a RADIUS server timeout:
**Requirements**

This example uses the following software and hardware components:

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

  **NOTE:** For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Set up a connection between the switch and the RADIUS server. See "*Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch*" on page 400.
- Configured users on the authentication server.

**Overview and Topology**

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, you configure alternative options for supplicants attempting LAN access. You can configure the switch to accept or deny access to supplicants or to maintain the access already granted to supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs.

*Figure 8 on page 410* shows the topology used for this example. The RADIUS server is connected to the EX4200 switch on access port **ge-0/0/10**. The switch acts as the authenticator port access entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks
all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface ge-0/0/1.

**NOTE:** This figure also applies to QFX5100 switches.

Figure 8: Topology for Configuring 802.1X Options

![Topology Diagram](image)

Table 25 on page 410 describes the components in this topology.

**Table 25: Components of the Topology**

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.</td>
</tr>
</tbody>
</table>
Table 25: Components of the Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN names</td>
<td>default VLAN</td>
</tr>
<tr>
<td></td>
<td>vlan-sf VLAN</td>
</tr>
<tr>
<td>Supplicant</td>
<td>Supplicant attempting access on interface ge-0/0/1</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, configure interface ge-0/0/1 to move a supplicant attempting access to the LAN during a RADIUS timeout to another VLAN. A RADIUS timeout prevents the normal exchange of EAP messages that carry information from the RADIUS server to the switch and permit the authentication of a supplicant. The default VLAN is configured on interface ge-0/0/1. When a RADIUS timeout occurs, supplicants on the interface will be moved from the default VLAN to the VLAN named vlan-sf.

Configuration

CLI Quick Configuration
To quickly configure server fail fallback on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit protocols dot1x authenticator]
set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Step-by-Step Procedure
To configure an interface to divert supplicants to a specific VLAN when a RADIUS timeout occurs (here, the VLAN is vlan-sf):

1. Define the VLAN to which supplicants are diverted:

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

Results
Display the results of the configuration:

```
user@switch> show configuration
interfaces {
```
ge-0/0/1 {
  unit 0 {
    family ethernet-switching {
      vlan {
        members default;
      }
    }
  }
  protocols {
    dot1x {
      authenticator {
        interface {
          ge-0/0/1.0 {
            server-fail vlan-name vlan-sf;
          }
        }
      }
    }
  }
}

Verification

IN THIS SECTION

- Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout | 412

To confirm that the configuration is working properly, perform these tasks:

**Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout**

**Purpose**
Verify that the interface moves supplicants to an alternative VLAN during a RADIUS timeout.

**NOTE:** On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.
Action

Display the VLANs configured on the switch; the interface ge-0/0/1.0 is a member of the default VLAN:

```
user@switch> show vlans

<table>
<thead>
<tr>
<th>Name</th>
<th>Tag</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td>ge-0/0/0.0, ge-0/0/1.0*, ge-0/0/5.0*, ge-0/0/10.0,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ge-0/0/12.0*, ge-0/0/14.0*, ge-0/0/15.0, ge-0/0/20.0</td>
</tr>
<tr>
<td>v2</td>
<td>77</td>
<td>None</td>
</tr>
<tr>
<td>vlan-sf</td>
<td>50</td>
<td>None</td>
</tr>
<tr>
<td>mgmt</td>
<td></td>
<td>me0.0*</td>
</tr>
</tbody>
</table>
```

Display 802.1X protocol information on the switch to view supplicants that are authenticated on interface ge-0/0/1.0:

```
user@switch> show dot1x interface brief

<table>
<thead>
<tr>
<th>802.1X Information:</th>
<th></th>
<th></th>
<th>MAC address</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Role</td>
<td>State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>Authenticator</td>
<td>Authenticated</td>
<td>00:00:00:00:00:01</td>
<td>abc</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/14.0</td>
<td>Authenticator</td>
<td>Connecting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/15.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/20.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

A RADIUS server timeout occurs. Display the Ethernet switching table to show that the supplicant with the MAC address 00:00:00:00:00:01 previously accessing the LAN through the default VLAN is now being learned on the VLAN named vlan-sf:

```
user@switch> show ethernet-switching table

<table>
<thead>
<tr>
<th>Ethernet-switching table: 3 entries, 1 learned</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>MAC address</td>
<td>Type</td>
<td>Age</td>
</tr>
<tr>
<td>v1</td>
<td>*</td>
<td>Flood</td>
<td></td>
</tr>
</tbody>
</table>
```
Display 802.1X protocol information to show that interface **ge-0/0/1.0** is connecting and will open LAN access to supplicants:

```
user@switch> show dot1x interface brief
```

### 802.1X Information:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>State</th>
<th>MAC address</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1.0</td>
<td>Authenticator</td>
<td>Connecting</td>
<td>00:00:00:00:00:01</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/14.0</td>
<td>Authenticator</td>
<td>Connecting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/15.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/20.0</td>
<td>Authenticator</td>
<td>Initialize</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**

The **show vlans** command displays interface **ge-0/0/1.0** as a member of the **default** VLAN. The **show dot1x interface brief** command shows that a supplicant (**abc**) is authenticated on interface **ge-0/0/1.0** and has the MAC address **00:00:00:00:00:01**. A RADIUS server timeout occurs, and the authentication server cannot be reached by the switch. The **show-ethernet-switching table** command shows that MAC address **00:00:00:00:00:01** is learned on VLAN **vlan-sf**. The supplicant has been moved from the **default** VLAN to the **vlan-sf** VLAN. The supplicant is then connected to the LAN through the VLAN named **vlan-sf**.

**SEE ALSO**

- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Configuring RADIUS Server Fail Fallback (CLI Procedure) | 384
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
- Understanding Server Fail Fallback and Authentication on Switches | 383
Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients

For 802.1X user authentication, EX Series switches support RADIUS authentication servers that are using Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) to authenticate Odyssey Access Client (OAC) supplicants. OAC networking software runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices) and provides secure access to both wired and wireless networks.

This example describes how to configure an 802.1X-enabled interface on the switch to provide fallback support for OAC users who have entered incorrect login credentials:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 11.2 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.
- One OAC end device acting as a supplicant.

Before you begin configuring the fallback option, ensure that you have:

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
• Configured EAP-TTLS on the server. See your RADIUS server documentation.
• Configured users on the RADIUS server. See your RADIUS server documentation.

Overview and Topology

OAC is networking software that runs on endpoint computers (desktop, laptop, or notepad) and supported wireless devices. OAC provides full support for EAP, which is required for secure wireless LAN access.

In this topology, OAC is deployed with an 802.1X-enabled switch and a RADIUS server. The switch functions as an enforcement point in the network security architecture. This topology:

• Ensures that only authorized users can connect.
• Maintains privacy of login credentials.
• Maintains data privacy over the wireless link.

This example includes the configuration of a server-reject VLAN on the switch, which can be used to prevent accidental lockout for users who have entered incorrect login credentials. These users can be given limited LAN access.

However, this fallback configuration is complicated by the fact that the OAC supplicant and RADIUS server are using EAP-TTLS. EAP-TTLS creates a secure encrypted tunnel between the server and the end device to complete the authentication process. When the user enters incorrect login credentials, the RADIUS server sends EAP failure messages directly to the client through this tunnel. The EAP failure message causes the client to restart the authentication procedure, so that the switch’s 802.1X authentication process tears down the session that was established with the switch using the server-reject VLAN. You can enable the remedial connection to continue by configuring:

• **eapol-block**—Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN. The block timer causes the authentication port access entity to ignore EAP start messages from the client, attempting to restart the authentication procedure.

  **NOTE:** The EAPoL block timer is triggered only after the configured number of allowed reattempts (using the **retries** option) on the 802.1X interface have been exhausted. You can configure **retries** to specify the number of times the switch attempts to authenticate the port after an initial failure. The default is three retries.

• **block-interval**—Configure the amount of time that you want the EAPoL block timer to continue to ignore EAP start messages. If you do not configure the block interval, the EAPoL block timer defaults to 120 seconds.

When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing remedial session that was established through the server-reject VLAN to remain open.
These configuration options apply to single, single-secure, and multiple supplicant authentication modes. In this example, the 802.1X interface is configured in single supplicant mode.

Figure 9 on page 417 shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.

NOTE: This figure also applies to QFX5100 switches.

Table 26 on page 417 describes the components in this OAC deployment:

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX Series switch</td>
</tr>
<tr>
<td>VLANs</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>server-reject-vlan: VLAN name is remedial and VLAN ID is 700</td>
</tr>
<tr>
<td>802.1X interface</td>
<td>ge-0/0/8</td>
</tr>
<tr>
<td>OAC supplicant</td>
<td>EAP-TTLS</td>
</tr>
<tr>
<td>One RADIUS authentication server</td>
<td>EAP-TTLS</td>
</tr>
</tbody>
</table>

Configuration

CLI Quick Configuration
To quickly configure the fallback options for EAP-TTLS and OAC supplicants, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set vlans remedial vlan-id 700
set protocols dot1x authenticator interface ge-0/0/8 retries 4
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan remedial
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan eapol-block
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130
```

**Step-by-Step Procedure**

To configure the fallback options for EAP-TTLS and OAC supplicants:

1. Configure a VLAN that will function as the server-reject VLAN to provide limited LAN access for users who have entered incorrect login credentials:

   ```plaintext
   user@switch# set vlans remedial vlan-id 700
   ```

2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

   ```plaintext
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set retries 4
   ```

3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

   ```plaintext
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set server-reject-vlan remedial
   ```

4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN.

   ```plaintext
   [edit protocols dot1x authenticator interface ge-0/0/8]
   ```
5. Configure the amount of time for the EAPoL block to remain in effect:

```
[edit protocols dot1x authenticator interface ge-0/0/8]
user@switch# set server-reject-vlan block-interval 130
```

**Results**

Check the results of the configuration:

```
user@switch> show configuration
protocols {
    dot1x {
        authenticator {
            interface {
                ge-0/0/8.0 {
                    supplicant single;
                    retries 4;
                    server-reject-vlan remedial block-interval 130 eapol-block;
                }
            }
        }
    }
}
```

**Verification**

To confirm that the configuration and the fallback options are working correctly, perform this task:

**Verifying the Configuration of the 802.1X Interface**

**Purpose**

Verify that the 802.1X interface is configured with the desired options.

**Action**

```
user@switch> show dot1x interface ge-0/0/8.0 detail
```
<table>
<thead>
<tr>
<th>ge-0/0/8.0</th>
<th>Role: Authenticator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrative state: Auto</td>
</tr>
<tr>
<td></td>
<td>Supplicant mode: Single</td>
</tr>
<tr>
<td></td>
<td>Number of retries: 4</td>
</tr>
<tr>
<td></td>
<td>Quiet period: 60 seconds</td>
</tr>
<tr>
<td></td>
<td>Transmit period: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Mac Radius: Disabled</td>
</tr>
<tr>
<td></td>
<td>Mac Radius Restrict: Disabled</td>
</tr>
<tr>
<td></td>
<td>Reauthentication: Enabled</td>
</tr>
<tr>
<td></td>
<td>Configured Reauthentication interval: 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Supplicant timeout: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Server timeout: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Maximum EAPoL requests: 2</td>
</tr>
<tr>
<td></td>
<td>Guest VLAN member: guest</td>
</tr>
<tr>
<td></td>
<td>Number of connected supplicants: 1</td>
</tr>
<tr>
<td></td>
<td>Supplicant: tem, 2A:92:E6:F2:00:00</td>
</tr>
<tr>
<td></td>
<td>Operational state: Authenticated</td>
</tr>
<tr>
<td></td>
<td>Backend Authentication state: Idle</td>
</tr>
<tr>
<td></td>
<td>Authentication method: Radius</td>
</tr>
<tr>
<td></td>
<td>Authenticated VLAN: remedial</td>
</tr>
<tr>
<td></td>
<td>Session Reauth interval: 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Reauthentication due in 68 seconds</td>
</tr>
</tbody>
</table>

**Meaning**

The `show dot1x ge-0/0/8 detail` command output shows that the ge-0/0/8 interface is in the **Authenticated** state and that it is using the **remedial** VLAN.

**SEE ALSO**

- [Understanding Authentication on Switches](#) | 361

---

**Monitoring 802.1X Authentication**

**Purpose**
NOTE: This topic applies only to the J-Web Application package.

J-Web Application package Release 14.1X53-A2 does not support 802.1X authentication on EX4600 switches.

Use the monitoring feature to display details of authenticated users and users that failed authentication.

**Action**

To display authentication details in the J-Web interface, select Monitoring > Security > 802.1X.

To display authentication details in the CLI, enter the following commands:

- `show dot1x interface detail | display xml`
- `show dot1x interface detail <interface> | display xml`
- `show dot1x auth-failed-users`

**Meaning**

The details displayed include:

- A list of authenticated users.
- The number of connected users.
- A list of users that failed authentication.

You can also specify an interface for which the details must be displayed.

**SEE ALSO**

- *Configuring 802.1X Authentication (J-Web Procedure)*
- *Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440*

### Verifying 802.1X Authentication

**Purpose**

Verify that supplicants are being authenticated on an interface on a switch with the interface configured for 802.1X authentication, and display the method of authentication being used.
Action

Display detailed information about an interface configured for 802.1X (here, the interface is ge-0/0/16):

```
user@switch> show dot1x interface ge-0/0/16.0 detail
```

```
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
      Reauthentication due in 17 seconds
```

Meaning

The sample output from the `show dot1x interface detail` command shows that the **Number of connected supplicants** is 1. The supplicant that was authenticated and is now connected to the LAN is known as **user5** on the RADIUS server and has the MAC address **00:30:48:8C:66:BD**. The supplicant was authenticated by means of the 802.1X authentication method called RADIUS authentication, as indicated by **Radius** in the output. When RADIUS authentication is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN **v200**.

Other 802.1X authentication methods supported on EX Series switches in addition to RADIUS authentication are:

- **Guest VLAN**—A nonresponsive host is granted Guest-VLAN access.
- **MAC Radius**—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server notifies the switch that the MAC
address is a permitted address, and the switch grants LAN access to the nonresponsive host on the interface to which it is connected.

- **Server-fail deny**—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from the supplicant from traversing through the interface. This is the default.

- **Server-fail permit**—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant were successfully authenticated by the RADIUS server.

- **Server-fail use-cache**—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted LAN access, but new supplicants are denied LAN access.

- **Server-fail VLAN**—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

**SEE ALSO**

- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring MAC RADIUS Authentication (CLI Procedure)
- Configuring RADIUS Server Fail Fallback (CLI Procedure)

## Troubleshooting Authentication of End Devices on EX Series Switches

**Problem**

**Description:** End devices configured using static MAC addresses lose connection to the switch after the clear dot1x interface command is run to clear all learned MAC addresses.

**Before clearing MAC addresses:**

```
user@switch# run show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned, 0 persistent entries
   VLAN      MAC address    Type       Age Interfaces
  vlan100       *           Flood       - All-members
     default       *           Flood       - All-members
     default    00:a0:d4:00:03:00  Learn       0 ge-3/0/16.0

user@switch> show dot1x authentication-bypassed-users
MAC address Interface      VLAN
00:a0:d4:00:03:00    ge-3/0/16.0  configured/default
```
To clear MAC addresses:

user@switch> clear dot1x interface

After clearing MAC addresses:

user@switch> show ethernet-switching table
Ethernet-switching table: 2 entries, 0 learned, 0 persistent entries

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC address</th>
<th>Type</th>
<th>Age</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan100</td>
<td>*</td>
<td>Flood</td>
<td>-</td>
<td>All-members</td>
</tr>
<tr>
<td>default</td>
<td>*</td>
<td>Flood</td>
<td>-</td>
<td>All-members</td>
</tr>
</tbody>
</table>

user@switch> show dot1x authentication-bypassed-users

Note that there are no end devices on the authentication bypass list.

**Cause**

Static MAC addresses are treated the same as other learned MAC addresses on an interface. When the clear dot1x interface command is run, it clears all learned MAC addresses from the interface, including the static MAC bypass list (also known as the exclusion list).

**Solution**

If you run the clear dot1x interfaces command for an interface that has static MAC addresses configured for authentication bypass, re-add the static MAC addresses to the static MAC bypass list.

**SEE ALSO**

- clear dot1x | 2477
- Understanding Authentication on Switches | 361
Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.4R1</td>
<td>Starting in Junos OS Release 18.3R1, you can configure 802.1X authentication on trunk interfaces, which allows the network access device (NAS) to authenticate an access point (AP) or another connected Layer 2 device.</td>
</tr>
<tr>
<td>17.3R1</td>
<td>Starting in Junos OS Release 17.3, the port bounce feature can be used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- RADIUS Server Configuration for Authentication | 378
- 802.1X and RADIUS Accounting | 434
- MAC RADIUS Authentication | 425
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

MAC RADIUS Authentication

IN THIS SECTION

- Configuring MAC RADIUS Authentication (CLI Procedure) | 426
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 427
You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network.

You can configure MAC RADIUS authentication on the switch interfaces to which the hosts are connected to provide LAN access. For more information, read this topic.

## Configuring MAC RADIUS Authentication (CLI Procedure)

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the switch interfaces to which the hosts are connected.

NOTE: You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPoL requests to the host. If there is no response from the host, the switch sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the `mac-radius restrict` option), the switch attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:
• Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.

To configure MAC RADIUS authentication by using the CLI:

• On the switch, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the restrict qualifier for interface ge-0/0/20 to have it use only MAC RADIUS authentication:

```
[edit]
user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

• On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f):

```
[root@freeradius]#
edi t /etc/raddb
vi users
00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"
```

SEE ALSO

| Understanding Authentication on Switches | 361 |

Example: Configuring MAC RADIUS Authentication on an EX Series Switch
To permit hosts that are not 802.1X-enabled to access a LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the switch will attempt to authenticate the host with the RADIUS server by using the host’s MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.3 or later for EX Series switches.
- An EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support or Example: Setting Up Basic Bridging and a VLAN on Switches. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
- Performed basic 802.1X configuration. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 390.

Overview and Topology

IEEE 802.1X port-based network access control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch by using the 802.1X protocol (that is, the devices are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC
RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is connected only to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication by using the `mac-radius restrict` option, and thus avoid the delay that occurs while the switch determines that the device is does not respond to EAP messages.

Figure 10 on page 430 shows the two printers connected to the switch.

**NOTE:** This figure also applies to QFX5100 switches.
Table 27 on page 430 shows the components in the example for MAC RADIUS authentication.

Table 27: Components of the MAC RADIUS Authentication Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 ports (ge-0/0/0 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>sales</td>
</tr>
<tr>
<td>Connections to printers (no PoE required)</td>
<td>ge-0/0/19, MAC address 00040ffdacfe</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/20, MAC address 0004aecd235f</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>Connected to the switch on interface ge-0/0/10</td>
</tr>
</tbody>
</table>

Figure 10: Topology for MAC RADIUS Authentication Configuration
The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the switch, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the switch attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the `mac radius restrict` option.

**Configuration**

**CLI Quick Configuration**

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/19 mac-radius
set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

**NOTE:** You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

**Step-by-Step Procedure**

Configure MAC RADIUS authentication on the switch and on the RADIUS server:

1. On the switch, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the restrict option on interface ge-0/0/20, so that only MAC RADIUS authentication is used:

   ```
   [edit]
   user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
   user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
   ```

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

   ```
   [root@freeradius]#
   edit /etc/raddb
   vi users
   00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
   0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
   ```
Results
Display the results of the configuration on the switch:

```
user@switch> show configuration protocols {
dot1x {
authenticator {
authentication-profile-name profile52;
interface {
ge-0/0/19.0 {
    mac-radius;
}
ge-0/0/20.0 {
    mac-radius {
        restrict;
    }
}
}
}
}
```

Verification

**IN THIS SECTION**

- Verifying That the Supplicants Are Authenticated | 432

Verify that the supplicants are authenticated:

**Verifying That the Supplicants Are Authenticated**

**Purpose**
After supplicants are configured for MAC RADIUS authentication on the switch and on the RADIUS server, verify that they are authenticated and display the method of authentication.

**Action**
Display information about the 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

```
user@switch> show dot1x interface ge-0/0/19.0 detail
```
ge-0/0/19.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
Supplicant: user101, 00:04:0f:fd:ac:fe
  Operational state: Authenticated
  Authentication method: Radius
  Authenticated VLAN: vo11
  Dynamic Filter: match source-dot1q-tag 10 action deny
  Session Reauth interval: 60 seconds
  Reauthentication due in 50 seconds

user@switch> show dot1x interface ge-0/0/20.0 detail

ge-0/0/20.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Enabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
Supplicant: user102, 00:04:ae:cd:23:5f
  Operational state: Authenticated
Meaning
The sample output from the `show dot1x interface detail` command displays the MAC address of the connected end device in the **Supplicant** field. On interface `ge-0/0/19`, the MAC address is `00:04:0f:fd:ac:fe`, which is the MAC address of the first printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **Radius**. On interface `ge-0/0/20`, the MAC address is `00:04:ae:cd:23:5f`, which is the MAC address of the second printer configured for MAC RADIUS authentication. The **Authentication method** field displays the authentication method as **Radius**.

**RELATED DOCUMENTATION**

- **Interfaces Enabled for 802.1X or MAC RADIUS Authentication | 456**
- **Static MAC Bypass of 802.1X and MAC RADIUS Authentication | 477**

**802.1X and RADIUS Accounting**

**IN THIS SECTION**

- Understanding 802.1X and RADIUS Accounting on Switches | 435
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438

EX Series Switches support RADIUS accounting. You can configure RADIUS accounting on an EX Series switch to collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The data gathered is used for network monitoring purpose.
Understanding 802.1X and RADIUS Accounting on Switches

Juniper Networks EX Series Ethernet Switches support IETF RFC 2866, RADIUS Accounting. By configuring RADIUS accounting on an EX Series switch, you can collect statistical data about users logging in to or out of a LAN and send that data to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based on the amount of time or type of services accessed.

RADIUS Accounting Process

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client forwards user accounting statistics to a designated RADIUS accounting server. The RADIUS accounting server must send a response to the client when it has successfully received and recorded the accounting statistics.

The RADIUS accounting process between a switch and a RADIUS server is based on the exchange of two types of RADIUS messages—Accounting-Request and Accounting-Response. Accounting-Request messages are sent from the switch to the server and convey information used to account for a service provided to a user. Accounting-Response messages are sent from the server to acknowledge receipt of the Accounting-Request packets. The exchange of messages between the switch and the server proceeds as follows:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. When a supplicant is authenticated through 802.1X authentication and then connected to the LAN, the switch forwards an Accounting-Request message with a record of the event to the accounting server. The Accounting-Request message sent by the switch includes the RADIUS attribute Acct-Status-Type with a value of Start, which indicates the beginning of user service for this supplicant. The accounting server records this event in the accounting log file as a start record.

3. The accounting server sends an Accounting-Response message back to the switch confirming that it received the accounting request. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.
4. The switch might send an interim message to the accounting server to periodically update the server with information pertaining to a specific session. Interim messages are sent as Accounting-Request messages with the Acct-Status-Type attribute value of Interim-Update. The accounting server sends an Accounting-Response message back to the switch to confirm receipt of an interim update.

5. When the supplicant’s session ends, the switch forwards an Accounting-Request message with the Acct-Status-Type attribute value set to Stop, indicating the end of user service. The accounting server records this event in the accounting log file as a stop record that contains session information and the length of the session.

The statistics collected through this process can be displayed from the RADIUS server. To view those statistics, the user needs to access the accounting log file configured to receive them. On FreeRADIUS, the filename is the server’s address—for example, 122.69.1.250.

**Supported RADIUS Attributes**

RADIUS accounting statistics are conveyed through the attributes included in each Accounting-Request message sent from the NAS to the server. Table 28 on page 436 list the RADIUS attributes supported for Accounting-Request messages.

**Table 28: RADIUS Accounting Request Attributes**

<table>
<thead>
<tr>
<th>Type</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>The name of the authenticated user.</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>The physical port number of the NAS that authenticates the user. Either NAS-Port or NAS-Port-ID must be contained in the packet.</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
<td>The IP address of the authenticated user.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The Framed-IP-Address attribute is sent only if a valid DHCP binding exists for the host in the DHCP snooping table.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Filter-ID</td>
<td>The name of the filter list for the user.</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
<td>The maximum transmission unit that can be configured for the user.</td>
</tr>
<tr>
<td>26</td>
<td>Client-System-Name</td>
<td>Vendor-specific attribute (VSA) used to indicate the client’s hostname.</td>
</tr>
<tr>
<td></td>
<td>Supported for LLDP-capable devices only.</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>Sets the maximum time (in seconds) that a session stays active before it terminates or a prompt is issued notifying its termination.</td>
</tr>
</tbody>
</table>
Table 28: RADIUS Accounting Request Attributes (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Idle-Timeout</td>
<td>The maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-ID</td>
<td>Enables the NAS to identify the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology.</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
<td>Enables the NAS to identify the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology.</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
<td>Contains a string identifying the NAS originating the Accounting-Request message.</td>
</tr>
<tr>
<td>40</td>
<td>Acct-Status-Type</td>
<td>Indicates whether this Accounting-Request message marks the beginning (Start) or the end (Stop) of the user session. Can also be used for an interim update (Interim-Update).</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
<td>A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file.</td>
</tr>
<tr>
<td>45</td>
<td>Acct-Authentic</td>
<td>Indicates whether the user was authenticated locally, by the RADIUS server, or by another remote authentication protocol.</td>
</tr>
<tr>
<td>55</td>
<td>Event-Timestamp</td>
<td>Records the time an event occurred.</td>
</tr>
<tr>
<td>87</td>
<td>NAS-Port-ID</td>
<td>Text string that identifies the port that authenticates the user. Either NAS-Port or NAS-Port-ID must be present in the packet.</td>
</tr>
</tbody>
</table>

SEE ALSO

- 802.1X for Switches Overview | 387
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
**Configuring 802.1X RADIUS Accounting (CLI Procedure)**

RADIUS accounting enables statistical data about users logging in to or out of a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used to perform general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

RADIUS accounting is based on a client/server model in which the switch, operating as the network access server (NAS), is the client. The client is responsible for forwarding user accounting statistics to a designated RADIUS accounting server. To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. If the primary server (the first one configured) is unavailable, then each RADIUS server in the list is tried in the order in which the servers are configured in Junos OS.

To configure RADIUS accounting by using the CLI:

1. Configure an access profile and specify the accounting servers to which the switch forwards accounting statistics:

   ```
   [edit access]
   user@switch# set profile profile-name radius accounting-server [server-addresses]
   ```

2. Define the address of RADIUS accounting servers and configure the secret password (the secret password on the switch must match the secret password on the server):

   ```
   [edit access]
   user@switch# set radius-server server-address secret password
   ```

3. Enable accounting for the access profile:

   ```
   [edit access]
   user@switch# set profile profile-name accounting
   ```

4. Configure the accounting order, making RADIUS the first method for sending accounting messages and updates:

   ```
   [edit access]
   user@switch# set profile profile-name accounting order radius
   ```

5. Configure the statistics to be collected on the switch and forwarded to the accounting server:

   ```
   [edit access]
   ```
user@switch# set profile profile-name accounting accounting-stop-on-access-deny
user@switch# set profile profile-name accounting accounting-stop-on-failure

6. (Optional) Configure the switch to send periodic updates for a user session at a specified interval to the accounting server:

   [edit access]
   user@switch# set profile profile-name accounting update-interval minutes

7. Display accounting statistics collected on the switch using the `show network-access aaa statistics accounting` command, for example:

   user@switch> show network-access aaa statistics accounting

   Accounting module statistics
   Requests received: 1
   Accounting Response failures: 0
   Accounting Response Success: 1
   Requests timedout: 0

8. Open an accounting log on the RADIUS accounting server by using the server's address, and view accounting statistics, for example:

   [root@freeradius]# cd /usr/local/var/log/radius/radacct/192.168.0.1
   [root@freeradius 192.168.0.1]# ls

   detail-20071214

   [root@freeradius 192.168.0.1]# vi details-20071214

   User-Name = "000347e1bab9"
   NAS-Port = 67
   Acct-Status-Type = Stop
   Acct-Session-Id = "802.1x811912"
   Acct-Input-Octets = 17454
   Acct-Output-Octets = 4245
   Acct-Session-Time = 1221041249
   Acct-Input-Packets = 72
   Acct-Output-Packets = 53
   Acct-Terminate-Cause = Lost-Carrier
   Acct-Input-Gigawords = 0
SEE ALSO

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400

RELATED DOCUMENTATION

RADIUS Server Configuration for Authentication | 378

Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch

IN THIS SECTION

- Requirements | 441
- Overview and Topology | 442
802.1x port-based network access control (PNAC) authentication on EX Series switches provides three types of authentication to meet the access needs of your enterprise LAN:

- Authenticate the first end device (supplicant) on an authenticator port, and allow all other end devices also connecting to have access to the LAN.
- Authenticate only one end device on an authenticator port at one time.
- Authenticate multiple end devices on an authenticator port. Multiple supplicant mode is used in VoIP configurations.

This example configures an EX Series switch to use IEEE 802.1X to authenticate end devices that use three different administrative modes.

**Requirements**

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from end devices until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for end devices (supplicants) that have permission to connect to the network.

Before you configure the ports for 802.1X authentication, be sure you have:

- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced
Layer 2 Software (ELS) configuration style, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support* or *Example: Setting Up Basic Bridging and a VLAN on Switches*. For all other switches, see *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

NOTE: For more about ELS, see *Using the Enhanced Layer 2 Software CLI*.

- Configured users on the authentication server.

### Overview and Topology

As shown in *Figure 11 on page 443*, the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.

NOTE: This figure also applies to QFX5100 switches.
Figure 11: Topology for Configuring Supplicant Modes

Authentication Server
RADIUS Server

IP Network

ge-0/0/10

ge-0/0/1

Conference room host

ge-0/0/11

ge-0/0/9

ge-0/0/8

PC

HUB

Supplicant (Client)

User 1, Password 1
User 2, Password 2
...
User n, Password n

Mac Address
00:04:aecd:23:5f

Mac Address
00:04:off:ff:ff

ge-0/0/20

ger-0/0/2

IP Telephone

PC
Table 29: Components of the Supplicant Mode Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>Connections to Avaya phones—with integrated hub, to connect phone and desktop PC to a single port; (requires PoE)</td>
<td>ge-0/0/8, ge-0/0/9, and ge-0/0/11</td>
</tr>
</tbody>
</table>

To configure the administrative modes to support supplicants in different areas of the Enterprise network:

- Configure access port ge-0/0/8 for single supplicant mode authentication.
- Configure access port ge-0/0/9 for single secure supplicant mode authentication.
- Configure access port ge-0/0/11 for multiple supplicant mode authentication.

**Single supplicant mode** authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

**Single-secure supplicant mode** authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.

**Multiple supplicant mode** authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

---

**Configuration of 802.1X to Support Multiple Supplicant Modes**

**CLI Quick Configuration**

To quickly configure the ports with different 802.1X authentication modes, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set protocols dot1x authenticator interface ge-0/0/8 supplicant single
set protocols dot1x authenticator interface ge-0/0/9 supplicant single-secure
set protocols dot1x authenticator interface ge-0/0/11 supplicant multiple
```
Step-by-Step Procedure
Configure the administrative mode on the interfaces:

1. Configure the supplicant mode as single on interface ge-0/0/8:

   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/8 supplicant single

2. Configure the supplicant mode as single secure on interface ge-0/0/9:

   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/9 supplicant single-secure

3. Configure multiple supplicant mode on interface ge-0/0/11:

   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/11 supplicant multiple

Results
Check the results of the configuration:

   [edit]
   user@access-switch> show configuration
protocols {
   dot1x {
      authenticator {
         interface {
            ge-0/0/8.0 {
               supplicant single;
            }
            ge-0/0/9.0 {
               supplicant single-secure;
            }
            ge-0/0/11.0 {
               supplicant multiple;
            }
         }
      }
   }
}
Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying the 802.1X Configuration

Purpose
Verify the 802.1X configuration on interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/5.

Action
Verify the 802.1X configuration by issuing the operational mode command `show dot1x interface`:

```
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>

user@switch> show dot1x interface ge-0/0/9.0 detail
ge-0/0/9.0
  Role: Authenticator
```
Administrative state: Auto
Supplicant mode: Single-Secure
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Disabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 0

user@switch> show dot1x interface ge-0/0/11.0 detail

ge-0/0/11.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Disabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 0

Meaning
The Supplicant mode output field displays the configured administrative mode for each interface. Interface ge-0/0/8.0 displays Single supplicant mode. Interface ge-0/0/9.0 displays Single-Secure supplicant mode. Interface ge-0/0/11.0 displays Multiple supplicant mode.

RELATED DOCUMENTATION
Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch

802.1X on EX Series switches provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as guests, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.
Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as a port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure guest VLAN authentication, be sure you have:

- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support or Example: Setting Up Basic Bridging and a VLAN on Switches. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

Overview and Topology

As part of IEEE 802.1X port-based network access control (PNAC), you can provide limited network access to supplicants who do not belong to a VLAN authentication group by configuring authentication for a guest VLAN. Typically, guest VLAN access is used to provide Internet access to visitors to a corporate site. However, you can also use the guest VLAN feature to provide access to a VLAN with limited resources to supplicants that fail 802.1X authentication on a corporate LAN.
NOTE: This figure also applies to QFX5100 switches.

Figure 12 on page 451 shows the conference room connected to the switch at interface ge-0/0/1.
Figure 12: Topology for Guest VLAN Example
Table 30: Components of the Guest VLAN Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (ge-0/0/0 through ge-0/0/7) and 16 non-PoE interfaces (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN names and tag IDs</td>
<td>sales, tag 100&lt;br&gt;support, tag 200&lt;br&gt;guest-vlan, tag 300</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database connected to the switch through interface ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, access interface ge-0/0/1 provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

### Configuration of a Guest VLAN That Includes 802.1X Authentication

#### CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans guest-vlan vlan-id 300
set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

#### Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on an EX Series switch:

1. Configure the VLAN ID for the guest VLAN:

```
[edit]
user@switch# set vlans guest-vlan vlan-id 300
```

2. Configure the guest VLAN under dot1x protocol:

```
[edit]
user@switch# set protocols dot1x authenticator interface all guest-vlan guest-vlan
```
Results
Check the results of the configuration:

```bash
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-vlan {
            guest-vlan;
          }
        }
      }
    }
  }
  vlans {
    guest-vlan {
      vlan-id 300;
    }
  }
}
```

Verification

**IN THIS SECTION**

- Verifying That the Guest VLAN Is Configured | 453

To confirm that the configuration is working properly, perform these tasks:

**Verifying That the Guest VLAN Is Configured**

**Purpose**
Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.
NOTE: On switches running Junos OS for EX Series with support for ELS, the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see Using the Enhanced Layer 2 Software CLI.

**Action**

Issue the operational mode commands:

```bash
user@switch> show vlans
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Tag</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td>ge-0/0/3.0*</td>
</tr>
<tr>
<td>dynamic</td>
<td>40</td>
<td>None</td>
</tr>
<tr>
<td>guest</td>
<td>30</td>
<td>None</td>
</tr>
<tr>
<td>guest-vlan</td>
<td>300</td>
<td>ge-0/0/1.0*</td>
</tr>
<tr>
<td>vlan_dyn</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

```bash
user@switch> show dot1x interface ge-0/0/1.0 detail
```

```
ge-0/0/1.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: guest-vlan
```
Number of connected supplicants: 1
Supplicant: user1, 00:00:00:00:13:23
   Operational state: Authenticated
   Authentication method: Radius
   Authenticated VLAN: vo11
   Dynamic Filter: match source-dot1q-tag 10 action deny
   Session Reauth interval: 60 seconds
   Reauthentication due in 50 seconds

Meaning
The output of the show vlans command shows guest-vlan as the VLAN name and the VLAN ID as 300.

The output of the show dot1x interface ge-0/0/1.0 detail command displays the Guest VLAN membership field, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the guest-vlan.

RELATED DOCUMENTATION
Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
Configuring 802.1X Interface Settings (CLI Procedure) | 390
Interfaces Enabled for 802.1X or MAC RADIUS Authentication

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes. Terms are applied after a device is successfully authenticated through 802.1X. For more information, read this topic.

Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants by Using RADIUS Server Attributes on an EX Series Switch

You can use RADIUS server attributes and a port firewall filter to centrally apply terms to multiple supplicants (end devices) connected to an EX Series switch in your enterprise. Terms are applied after a device is
successfully authenticated through 802.1X. If the firewall filter configuration is modified after end devices are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter changes to take effect.

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they must be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server by using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For information about configuring your server, consult the documentation that was included with your RADIUS server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

**Requirements**

This example uses the following software and hardware components:

**NOTE:** This example also applies to QFX5100 switches.

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
- Configured 802.1X authentication on the switch, with the supplicant mode for interface ge-0/0/2 set to multiple. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 390 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 440.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).
Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, you can apply a single port firewall filter configured through the Junos OS CLI on the EX Series switch to any number of end devices (supplicants) by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate end devices.

For more information about firewall filters, see Firewall Filters for EX Series Switches Overview or Overview of Firewall Filters.

RADIUS server attributes are applied to the port where the end device is connected after the device is successfully authenticated using 802.1X. To authenticate an end device, the switch forwards the end device's credentials to the RADIUS server. The RADIUS server matches the credentials against preconfigured information about the supplicant located in the supplicant's user profile on the RADIUS server. If a match is found, the RADIUS server instructs the switch to open an interface to the end device. Traffic then flows from and to the end device on the LAN. Further instructions configured in the port firewall filter and added to the end device’s user profile using a RADIUS server attribute further define the access that the end device is granted. Filtering terms configured in the port firewall filter are applied to the port where the end device is connected after 802.1X authentication is complete.

NOTE: If you modify the port firewall filter after an end device is successfully authenticated using 802.1X, you must terminate and re-establish the 802.1X authentication session for the firewall filter configuration changes to be effective.

Figure 13 on page 459 shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port ge-0/0/10. Two end devices (supplicants) are accessing the LAN on interface ge-0/0/2. Supplicant 1 has the MAC address 00:50:8b:6f:60:3a. Supplicant 2 has the MAC address 00:50:8b:6f:60:3b.

NOTE: This figure also applies to QFX5100 switches.
Figure 13: Topology for Firewall Filter and RADIUS Server Attributes Configuration

Table 31 on page 459 describes the components in this topology.

Table 31: Components of the Firewall Filter and RADIUS Server Attributes Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports: 16 non-PoE ports and 8 PoE ports.</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with the address <strong>10.0.0.100</strong> connected to the switch at port <strong>ge-0/0/10</strong>.</td>
</tr>
</tbody>
</table>
Table 31: Components of the Firewall Filter and RADIUS Server Attributes Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
</table>
| 802.1X supplicants connected to the switch on interface ge-0/0/2 | • Supplicant 1 has MAC address 00:50:8b:6f:60:3a.  
• Supplicant 2 has MAC address 00:50:8b:6f:60:3b. |
| Port firewall filter to be applied on the RADIUS server | filter1                                                                 |
| Counters                                           | counter1 counts packets from Supplicant 1, and counter2 counts packets from Supplicant 2. |
| Policer                                            | policer p1                                                               |
| User profiles on the RADIUS server                 | • Supplicant 1 has the user profile supplicant1.  
• Supplicant 2 has the user profile supplicant2. |

In this example, you configure a port firewall filter named filter1. The filter contains terms that will be applied to the end devices based on the MAC addresses of the end devices. When you configure the filter, you also configure the counters counter1 and counter2. Packets from each end device are counted, which helps you verify that the configuration is working. Policer p1 limits the traffic rate based on the values for exceeding and discard parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

Configuring the Port Firewall Filter and Counters

CLI Quick Configuration
To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]

set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```
set firewall family ethernet-switching filter filter1 term supplicant1 then count counter1
set firewall family ethernet-switching filter filter1 term supplicant1 then policer p1
set firewall family ethernet-switching filter filter1 term supplicant2 then count counter2

Step-by-Step Procedure
To configure a port firewall filter and counters on the switch:

1. Configure a port firewall filter (here, filter1) with terms for each end device based on the MAC address of each end device:

[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
user@switch# set filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b

2. Set policer definition:

[edit]
user@switch# set firewall policer p1 if-exceeding bandwidth-limit 1m
user@switch# set firewall policer p1 if-exceeding burst-size-limit 1k
user@switch# set firewall policer p1 then discard

3. Create two counters that will count packets for each end device and a policer that limits the traffic rate:

[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 then count counter1
user@switch# set filter filter1 term supplicant1 then policer p1
user@switch# set filter filter1 term supplicant2 then count counter2

Results
Display the results of the configuration:

```
user@switch> show configuration
firewall{
    family ethernet-switching{
        filter filter1{
            term supplicant1{
                from{
                    source-mac-address{
                        00:50:8b:6f:60:3a;
```
Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

Step-by-Step Procedure
To verify that the RADIUS server attribute Filter-ID is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary dictionary.rfc2865 on the RADIUS server, and verify that the attribute Filter-ID is in the dictionary:

   [root@freeradius]# cd /usr/share/freeradius/dictionary.rfc2865

2. Close the dictionary file.

3. Display the local user profiles of the end devices to which you want to apply the filter (here, the user profiles are called supplicant1 and supplicant2):

   [root@freeradius]# cat /usr/local/etc/raddb/users

   The output shows:
supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-Id = "1005"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-Id = "1005"

4. Apply the filter to both user profiles by adding the line Filter-Id = "filter1" to each profile, and then close the file:

   [root@freeradius]# cat /usr/local/etc/raddb/users

After you paste the line into the files, the files look like this:

supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-Id = "1005",
  Filter-Id = "filter1"

supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-Id = "1005",
  Filter-Id = "filter1"

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose
After the end devices are authenticated on interface ge-0/0/2, verify that the filter has been configured on the switch and includes the results for both supplicants:

Action

user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/2

Counters
counter1_dot1x_ge-0/0/2_user1 100
counter2_dot1x_ge-0/0/2_user2 400

Meaning
The output of the show dot1x firewall command displays counter1 and counter2. Packets from User_1 are counted using counter1, and packets from User 2 are counted using counter2. The output displays packets incrementing for both counters. The filter has been applied to both end devices.

SEE ALSO
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
- Understanding Authentication on Switches | 361
- Understanding Dynamic Filters Based on RADIUS Attributes | 405

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS
server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- One EX Series switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.
- Configured 802.1X authentication on the switch, with the authentication mode for interface ge-0/0/2 set to **multiple**. See "Configuring 802.1X Interface Settings (CLI Procedure)" on page 390 and "Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch" on page 440.
- Configured users on the RADIUS authentication server.

**Overview and Topology**

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 14 on page 466, when User1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

**NOTE:** If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. **Figure 15 on page 467** shows the network topology for this example.
To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

**Configuring Firewall Filters on Interfaces with Multiple Supplicants**

**CLI Quick Configuration**

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/2 supplicant multiple
```
Step-by-Step Procedure
To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface ge-0/0/2 for multiple supplicant mode authentication:

   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/2 supplicant multiple

2. Set policer definition:

   user@switch# show policer p1 |display set
   set firewall policer p1 if-exceeding bandwidth-limit 1m
   set firewall policer p1 if-exceeding burst-size-limit 1k
   set firewall policer p1 then discard

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

   [edit firewall family ethernet-switching]
   user@switch# set filter filter1 term term1 from destination-address 192.0.2.16/28
   user@switch# set filter filter1 term term1 then count counter1
   user@switch# set filter filter1 term term2 then policer p1

Results
Check the results of the configuration:

   user@switch> show configuration

   firewall {
      family ethernet-switching {
         filter filter1 {
            term term1 {
   

from {
    destination-address {
        192.0.2.16/28;
    }
}
then count counter1;
term term2 {
    from {
        destination-address {
            192.0.2.16/28;
        }
    }
    then policer p1;
}
policer p1 {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 1k;
    }
    then discard;
}
protocols {
    dot1x {
        authenticator
        interface ge-0/0/2 {
            supplicant multiple;
        }
    }
}

Verification

IN THIS SECTION

- Verifying Firewall Filters on Interfaces with Multiple Supplicants | 470

To confirm that the configuration is working properly, perform these tasks:
**Verifying Firewall Filters on Interfaces with Multiple Supplicants**

**Purpose**
Verify that firewall filters are functioning on the interface with multiple supplicants.

**Action**
1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on `ge-0/0/2`:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User2, is authenticated on the same interface, `ge-0/0/2`, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   counter1_dot1x_ge-0/0/2_user2 400
   ```

**Meaning**
The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

**SEE ALSO**

- *Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches*
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on EX Series Switches with ELS Support

IN THIS SECTION

- Requirements | 471
- Overview and Topology | 472
- Configuration | 474
- Verification | 476

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication" on page 464. For ELS details, see Using the Enhanced Layer 2 Software CLI.

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2 or later for EX Series switches
• One EX Series switch with support for ELS

• One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

• Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.

• Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to multiple. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 390 and “Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch” on page 440.

• Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 16 on page 473, when User 1 is authenticated by the EX Series switch, the system adds a term to the firewall filter dynamic-filter-example. When User 2 is authenticated, another term is added to the firewall filter, and so on.

NOTE: This figure also applies to QFX5100 switches.
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

**NOTE:** If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. *Figure 17 on page 474* shows the network topology for this example.
Configuration

Configuring Firewall Filters on Interfaces with Multiple Supplicants

CLI Quick Configuration
To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term term1 from ip-destination-address 192.0.2.16/28
set firewall family ethernet-switching filter filter1 term term2 from ip-destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```
Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Set the policer definition:

```bash
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```

2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```bash
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

Results

Check the results of the configuration:

```bash
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
            then count counter1;
            term term2 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
            then policer p1;
```

```
Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose
Verify that firewall filters are functioning on the interface with multiple supplicants.

Action
1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2:

   ```
   user@switch> show dot1x firewall
   
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@switch> show dot1x firewall
   ```
Meaning
The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address 100 times, while User 2 accessed the same file server 400 times.

SEE ALSO

* Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

* Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395

RELATED DOCUMENTATION

* Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440

Static MAC Bypass of 802.1X and MAC RADIUS Authentication

Junos OS allows you to configure access to your LAN through 802.1X-configured interfaces without authentication, by configuring a static MAC bypass list on the EX Series switch. The static MAC bypass
Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication (CLI Procedure)

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

  ```
  [edit protocols dot1x]
  user@switch# set authenticator static 00:04:0f:fd:ac:fe
  ```

- Configure a supplicant to bypass authentication if it is connected through a particular interface:

  ```
  [edit protocols dot1x]
  user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5
  ```

- Configure a supplicant to be moved to a specific VLAN after it is authenticated:

  ```
  [edit protocols dot1x]
  user@switch# set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment default-vlan
  ```

SEE ALSO

- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring 802.1X Authentication (J-Web Procedure)
Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the exclusion list, specifies MAC addresses that are allowed on the switch without sending a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you configure static MAC bypass of authentication, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see Example: Setting Up Basic Bridging and a VLAN for an EX
Series Switch with ELS Support or Example: Setting Up Basic Bridging and a VLAN on Switches. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

For more about ELS, see: Using the Enhanced Layer 2 Software CLI.

- Specified the RADIUS server connections and configured an access profile on the switch. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.

**Overview and Topology**

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Figure 18 on page 481 shows the two printers connected to the EX4200.

**NOTE:** This figure also applies to QFX5100 switches.
The interfaces shown in Table 32 on page 482 will be configured for static MAC bypass of authentication.
The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface ge-0/0/19. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface ge-0/0/20. Both printers will be added to the static list and bypass 802.1X authentication.

Configuration

CLI Quick Configuration
To quickly configure the static MAC bypass list, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols dot1x authenticator interface all supplicant multiple
set protocols dot1x authenticator authenticaton-profile-name profile1
```

Step-by-Step Procedure
Configure the static MAC bypass list:

1. Configure MAC addresses 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f as static MAC addresses:

```
[edit protocols]
user@switch# set dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
```

2. Configure the 802.1X authentication method:

```
[edit protocols]
user@switch# set dot1x authenticator interface all supplicant multiple
```

3. Configure the authentication profile name (access profile name) to use for authentication:

```
[edit protocols]
user@switch# set dot1x authenticator authentication-profile-name profile1
```
**Results**

Display the results of the configuration:

```plaintext
user@switch> show
interfaces {
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
  ge-0/0/20 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
}
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile1
      static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
      interface {
        all {
          supplicant multiple;
        }
      }
    }
  }
}
```
Verification

To confirm that the configuration is working properly, perform these tasks:

**Verifying Static MAC Bypass of Authentication**

**Purpose**
Verify that the MAC addresses of both printers are configured and associated with the correct interfaces.

**Action**
Issue the operational mode command:

```
user@switch> show dot1x static-mac-address
```

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:0f:fd:ac:fe</td>
<td>default</td>
<td>ge-0/0/19.0</td>
</tr>
<tr>
<td>00:04:ae:cd:23:5f</td>
<td>default</td>
<td>ge-0/0/20.0</td>
</tr>
</tbody>
</table>

**Meaning**
The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

**SEE ALSO**

- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Understanding Authentication on Switches | 361
Captive Portal Authentication

You can control access to your network through a switch by using several different authentication. Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. You can set up captive portal authentication on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. For more information, read this topic.

Example: Setting Up Captive Portal Authentication on an EX Series Switch

IN THIS SECTION

- Requirements | 486
- Overview and Topology | 486
- Configuration | 486
- Verification | 490
- Troubleshooting | 491
You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

**Requirements**

This example uses the following hardware and software components:

- An EX Series switch that supports captive portal
- Junos OS Release 10.1 or later for EX Series switches

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
- Generated an SSL certificate and installed it on the switch. See “Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)” on page 341.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 494.

**Overview and Topology**

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication whitelist. The MAC addresses in this list are permitted access on the interface without captive portal.

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

**Configuration**

To configure captive portal on your switch:

**CLI Quick Configuration**

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
```
set access radius-server 10.204.96.165 port 1812
set access radius-server 10.204.96.165 secret "ABC123"
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server 10.204.96.165
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set services captive-portal authentication-profile-name profile1
set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
set services captive-portal custom-options post-authentication-url http://www.my-home-page.com

Step-by-Step Procedure
To configure captive portal on the switch:

1. Define the server IP address, the server authentication port number, and configure the secret password. The secret password on the switch must match the secret password on the server:

   [edit]
   user@switch# set access radius-server 10.204.96.165 port 1812
   [edit]
   user@switch# set access radius-server 10.204.96.165 secret "ABC123"

2. Configure the authentication order, making radius the first method of authentication:

   [edit]
   user@switch# set access profile profile1 authentication-order radius

3. Configure the server IP address to be tried in order to authenticate the supplicant:

   [edit]
   user@switch# set access profile profile1 radius authentication-server 10.204.96.165

4. Enable HTTP access on the switch:

   [edit]
   user@switch# set system services web-management http

5. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:
NOTE: You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

a. Associate the security certificate with the Web server and enable HTTPS access on the switch:

```plaintext
[edit]
user@switch# set system services web-management https local-certificate my-signed-cert
```

b. Configure captive portal to use HTTPS:

```plaintext
[edit]
user@switch# set services captive-portal secure-authentication https
```

6. Enable an interface for captive portal:

```plaintext
[edit]
user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
```

7. Specify the name of the access profile to be used for captive portal authentication:

```plaintext
[edit]
user@switch# set services captive-portal authentication-profile-name profile1
```

8. (Optional) Allow specific clients to bypass captive portal:

```plaintext
[edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.
NOTE: Optionally, you can use set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0 to limit the scope to the interface.

9. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

[edit]
user@switch# set services captive-portal custom-options post-authentication-url http://www.my-home-page.com

Results
Display the results of the configuration:

[edit]
user@switch> show system {
    services {
        web-management {
            http;
            https {
                local-certificate my-signed-cert;
            }
        }
    }
    security {
        certificates {
            local {
                my-signed-cert {
                    "-----BEGIN RSA PRIVATE KEY-----ABC123
                    ...
                    ABC123-----END CERTIFICATE-----\n"; ## SECRET-DATA
                }
            }
        }
        services {
            captive-portal {
                interface {
                    ge-0/0/10.0 {
                    }
To confirm that captive portal is configured and working properly, perform these tasks:

**Verifying That Captive Portal Is Enabled on the Interface**

**Purpose**

Verify that captive portal is configured on interface ge-0/0/10.

**Action**

Use the operational mode command `show captive-portal interface interface-name detail`:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
```

```
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```
Meaning
The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose
Verify that captive portal is working on the switch.

Action
Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

To troubleshoot captive portal, perform these tasks:

Troubleshooting Captive Portal

Problem
The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a Web page.

Solution
You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

user@switch> show captive-portal firewall ge-0/0/10.0

ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name      Bytes      Packets

Configuring Captive Portal Authentication (CLI Procedure)

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a web page, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
- Generated an SSL certificate and installed it on the switch. See "Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)" on page 341.
- Configured basic access between the EX Series switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.
- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 494.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal | 492
- Enabling an Interface for Captive Portal | 493
- Configuring Bypass of Captive Portal Authentication | 493

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Enable HTTP access on the switch:

   [edit]
user@switch# set system services web-management http

2. Associate the security certificate with the Web server and enable HTTPS access on the switch:

    [edit]
user@switch# set system services web-management https local-certificate my-signed-cert

NOTE: You can enable HTTP without HTTPS, but we recommend HTTPS for security purposes.

3. Configure captive portal to use HTTPS:

    [edit]
user@switch# set services captive-portal secure-authentication https

Enabling an Interface for Captive Portal

To enable an interface for captive portal:

    [edit]
user@switch# set services captive-portal interface interface-name

For example, to enable captive portal on the interface ge-0/0/10:

    [edit]
user@switch# set services captive-portal interface ge-0/0/10

Configuring Bypass of Captive Portal Authentication

To allow specific clients to bypass captive portal:

    [edit]
user@switch# set ethernet-switching-options authentication-whitelist mac-address

For example, to allow specific clients to bypass captive portal:

    [edit]
user@switch# set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22
NOTE: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and authentication bypass will not be allowed.

Designing a Captive Portal Authentication Login Page on Switches

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires users to input a username and password before they are allowed access. Upon successful authentication, users are allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the terms and conditions of use. By clicking the Agree button, the user can access the captive portal login page.

*Figure 19 on page 495* shows an example of a captive portal login page:
Table 33 on page 495 summarizes the configurable elements of a captive portal login page.

**Table 33: Configurable Elements of a Captive Portal Login Page**

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footer background color</td>
<td>footer-bgc hex-color</td>
<td>The HTML hexadecimal code for the background color of the captive portal login page footer.</td>
</tr>
<tr>
<td>Footer message</td>
<td>footer-message text-string</td>
<td>Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy. The default text shown in the footer is Copyright @2010, Juniper Networks Inc.</td>
</tr>
<tr>
<td>Footer text color</td>
<td>footer-text-color</td>
<td>Color of the text in the footer. The default color is white.</td>
</tr>
<tr>
<td>Form header background color</td>
<td>form-header-bgc hex-color</td>
<td>The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.</td>
</tr>
<tr>
<td>Form header message</td>
<td>form-header-message text-string</td>
<td>Text displayed in the header of the captive portal login page. The default text is Captive Portal User Authentication.</td>
</tr>
<tr>
<td>Form header text color</td>
<td>form-header-text-color color</td>
<td>Color of the text in the form header. The default color is black.</td>
</tr>
</tbody>
</table>
To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

   `user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg`

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

   ```
   [edit system services captive-portal]
   user@switch# set custom-options header-bgc color #006600
   set custom-options header-message "Welcome to Our Network"
   set custom-options banner-message "Please enter your username and password". The banner displays the message "XXXXXXX" by default. The user can modify this message.
   ```

### Table 33: Configurable Elements of a Captive Portal Login Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form reset button label</td>
<td>form-reset-label name</td>
<td>Using the Reset button, the user can clear the username and password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fields on the form.</td>
</tr>
<tr>
<td>Form submit button label</td>
<td>form-submit-label name</td>
<td>Using the Login button, the user can submit the login information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header background color</td>
<td>header-bgc color</td>
<td>The HTML hexadecimal code for the background color of the captive portal</td>
</tr>
<tr>
<td></td>
<td>uel name</td>
<td>login page header.</td>
</tr>
<tr>
<td>Header logo</td>
<td>header-logo filename</td>
<td>Filename of the file containing the image of the logo that you want to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>appear in the header of the captive portal login page. The image file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>can be in GIF, JPEG, or PNG format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can upload a logo image file to the switch. Copy the logo to the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/var/tmp directory on the switch (during commit, the files are saved to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>persistent locations).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not specify a logo image, the Juniper Networks logo is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>displayed.</td>
</tr>
<tr>
<td>Header message</td>
<td>header-message text-string</td>
<td>Text displayed in the page header. The default text is User Authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header text color</td>
<td>header-text-color color</td>
<td>Color of the text in the header. The default color is white.</td>
</tr>
<tr>
<td>Post-authentication URL</td>
<td>post-authentication-url url</td>
<td>URL to which the users are directed on successful authentication. By default,</td>
</tr>
<tr>
<td></td>
<td>url</td>
<td>users are directed to the page they had originally requested.</td>
</tr>
</tbody>
</table>
Now you can commit the configuration.

NOTE: For the custom options that you do not specify, the default value is used.

SEE ALSO

- Understanding Authentication on Switches | 361
- captive-portal | 1554

Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switch with ELS Support

NOTE: This task uses Junos OS for switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see “Configuring Captive Portal Authentication (CLI Procedure)” on page 492. For ELS details, see Using the Enhanced Layer 2 Software CLI.

Configure captive portal authentication (hereafter referred to as captive portal) on a switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support.
- Generated an SSL certificate and installed it on the switch. See “Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)” on page 341.
- Configured basic access between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.

- Designed your captive portal login page. See "Designing a Captive Portal Authentication Login Page on Switches" on page 494.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal | 498
- Enabling an Interface for Captive Portal | 498
- Configuring Bypass of Captive Portal Authentication | 498

**Configuring Secure Access for Captive Portal**

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

   ```
   [edit]
   user@switch# set system services web-management https local-certificate certificate-name
   ```

   **NOTE:** You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@switch# set services captive-portal secure-authentication https
   ```

**Enabling an Interface for Captive Portal**

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface interface-name
```
NOTE: Optionally, you can use `set switch-options authentication-whitelist mac-address` interface `interface-name` to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address session-mac-addr` command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address is not added to the Ethernet switching table and the authentication bypass is not allowed.

Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon
successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an EX Series switch:

**Requirements**

This example uses the following software and hardware components:

- Junos OS Release 13.2X50 or later for EX Series switches
- An EX Series switch with support for ELS

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support*.
- Generated an SSL certificate and installed it on the switch. See “Generating SSL Certificates to Be Used for Secure Web Access (EX Series Switch)” on page 341.
- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
- Designed your captive portal login page. See “Designing a Captive Portal Authentication Login Page on Switches” on page 494.

**Overview and Topology**

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN, add its MAC address to the authentication whitelist and assign it to a VLAN, vlan1. The MAC addresses on this list are permitted access on the interface without captive portal authentication.

The topology for this example consists of one EX Series switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

**Configuration**

To configure captive portal on your switch:

**CLI Quick Configuration**

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
```
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
set custom-options post-authentication-url http://www.my-home-page.com

Step-by-Step Procedure

1. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:
   a. Associate the security certificate with the Web server and enable HTTPS on the switch:

   ```bash
   [edit]
   user@switch# set system services web-management https local-certificate my-signed-cert
   
   NOTE: You can enable HTTP instead of HTTPS, but we recommend that you enable HTTPS for security purposes.
   ```

   b. Configure captive portal to use HTTPS:

   ```bash
   [edit]
   user@switch# set services captive-portal secure-authentication https
   ```

2. Enable an interface for captive portal:

   ```bash
   [edit]
   user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
   ```

3. (Optional) Allow specific clients to bypass captive portal authentication:

   ```bash
   [edit]
   user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
   
   NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the clear captive-portal mac-address mac-address command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.
   ```
4. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

[edit services captive-portal]
user@switch# set custom-options post-authentication-url http://www.my-home-page.com

Results
Display the results of the configuration:

```
[edit]
user@switch# show
system {
  services {
    web-management {
      https {
        local-certificate my-signed-cert;
      }
    }
  }
}
security {
  certificates {
    local {
      my-signed-cert {
        "-----BEGIN RSA PRIVATE KEY-----\ABC123
        ABC123ABC123ABC123 ... ABC123
        ----END CERTIFICATE-----\n"; ## SECRET-DATA
      }
    }
  }
}
services {
  captive-portal {
    interface {
      ge-0/0/10.0 {
        supplicant multiple;
      }
    }
  }
```
To confirm that captive portal authentication is configured and working properly, perform these tasks:

**Verifying That Captive Portal Is Enabled on the Interface**

**Purpose**

Verify that captive portal is configured on the interface ge-0/0/10.

**Action**

Use the operational mode command `show captive-portal interface interface-name detail`:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
```

```
ge-0/0/10.0
    Supplicant mode: Multiple
    Number of retries: 3
    Quiet period: 60 seconds
    Configured CP session timeout: 3600 seconds
    Server timeout: 15 seconds
```
Meaning
The output confirms that captive portal is configured on the interface ge-0/0/10, with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose
Verify that captive portal is working on the switch.

Action
Connect a client to the interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

IN THIS SECTION
- Troubleshooting Captive Portal | 504

To troubleshoot captive portal, perform this task:

Troubleshooting Captive Portal

Problem
The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.

Solution
You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

user@switch> show captive-portal firewall ge-0/0/10.0

ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10

Counters:
Name      Bytes      Packets

RELATED DOCUMENTATION

Flexible Authentication Order on EX Series Switches | 505
Central Web Authentication | 510
Centralized Access Control to Network Resources on EX Series Switches | 517

Flexible Authentication Order on EX Series Switches

IN THIS SECTION

- Configuring Flexible Authentication Order | 506
- Configuring EAPoL Block to Maintain an Existing Authentication Session | 508

Junos OS switches support 802.1X, MAC RADIUS, and captive portal as an authentication methods to devices requiring to connect to a network. You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. For more information, read this topic.
**Configuring Flexible Authentication Order**

You can use the flexible authentication order feature to specify the order of authentication methods that the switch uses when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch will attempt authentication using MAC RADIUS. If MAC RADIUS fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

With a flexible authentication order, the sequence of authentication method used can be changed based on the type of clients connected to the interface. You can configure the `authentication-order` statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried. Captive portal is always the last authentication method tried.

If MAC RADIUS authentication is configured as the first authentication method in the order, then on receiving data from any client, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch uses 802.1X authentication to authenticate the client. If 802.1X authentication fails, and captive portal is configured on the interface, the switch attempts authentication using captive portal.

**NOTE:** If 802.1X authentication and MAC RADIUS authentication fail, and captive portal is not configured on the interface, the client is denied access to the LAN unless a server fail fallback method is configured. See “Configuring RADIUS Server Fail Fallback (CLI Procedure)” on page 384 for more information.

Different authentication methods can be used in parallel on an interface that is configured in multiple-suppliant mode. Therefore, if an end device is authenticated on the interface by using captive portal, another end device connected to that interface can still be authenticated using 802.1X or MAC RADIUS authentication.

Before you configure the flexible authentication order on an interface, make sure that the authentication methods are configured on that interface. The switch does not attempt authentication using a method that is not configured on the interface, even if that method is included in the authentication order; the switch ignores that method and attempts the next method in the authentication order that is enabled on that interface.
Use the following guidelines when configuring the `authentication-order` statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If `mac-radius-restrict` is configured on an interface then the authentication order cannot be configured on that interface.

To configure a flexible authentication order, use one of the following valid combinations:

```
NOTE: The authentication order can be configured globally using the `interface all` option as well as locally using the individual interface name. If the authentication order is configured both for an individual interface and for all interfaces, the local configuration for that interface overrides the global configuration.
```

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication, and then captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x mac-radius captive-portal]
  ```

- To configure 802.1X authentication as the first authentication method, followed by captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x captive-portal]
  ```

- To configure 802.1X authentication as the first authentication method, followed by MAC RADIUS authentication:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [dot1x mac-radius]
  ```

- To configure MAC RADIUS authentication as the first authentication method, followed by 802.1X, followed by captive portal:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name authentication-order
  [mac-radius dot1x captive-portal]
  ```
After you configure the authentication order, you must use the **insert** command to make any modifications to the authentication order. Using the **set** command does not change the configured order.

To change the authentication order after initial configuration:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order authentication-method before authentication-method
```

For example, to change the order from `[mac-radius dot1x captive portal]` to `[dot1x mac-radius captive portal]`:

```
[edit]
user@switch# insert protocols dot1x authenticator interface interface-name authentication-order dot1x before mac-radius
```

**SEE ALSO**

- **Understanding Authentication on Switches** | 361
- **Example: Configuring MAC RADIUS Authentication on an EX Series Switch** | 427

---

### Configuring EAPoL Block to Maintain an Existing Authentication Session

When a switch acting as an 802.1X authenticator receives an EAP-Start message from an authenticated client, the switch tries to re-authenticate the client using the 802.1X method and typically returns an EAP-Request message, and waits for a response. If the client fails to respond, the switch attempts to re-authenticate the client using MAC RADIUS or captive portal method if these methods were configured. Clients that have been authenticated using MAC RADIUS or captive portal authentication are non-responsive, and traffic is dropped on the interface as the switch attempts re-authentication.

If you have configured flexible authentication order on the interface so that MAC RADIUS is the first method used to authenticate a client, the switch still reverts to using 802.1X for re-authentication if the client sends an EAP-Start message, even if the client was successfully authenticated using MAC RADIUS authentication. You can configure an EAPoL block with either a fixed or flexible authentication order. If you do not configure the `authentication-order` statement, the order is fixed by default. The `eapol-block` statement can be configured with or without configuring the `authentication-order` statement.

You can configure a switch to ignore EAP-Start messages sent from a client that has been authenticated using MAC RADIUS authentication or captive portal authentication using the `eapol-block` statement. With
a block of EAPoL messages in effect, if the switch receives an EAP-Start message from the client, it does not return an EAP-Request message, and the existing authentication session is maintained.

**NOTE:** If the endpoint has not been authenticated with MAC RADIUS authentication or captive portal authentication, the EAPoL block does not take effect. The endpoint can authenticate using 802.1X authentication.

If `eapol-block` is configured with the `mac-radius` option, then once the client is authenticated with MAC RADIUS authentication or CWA (Central Web Authentication), the client remains in authenticated state even if it sends an EAP-Start message. If `eapol-block` is configured with the `captive-portal` option, then once the client is authenticated with captive portal, the client remains in authenticated state even if it sends an EAP-Start message.

**NOTE:** This feature is supported on EX4300 and EX9200 switches.

To configure a block of EAPoL messages to maintain an existing authentication session:

- To configure EAPoL block for a client authenticated using MAC RADIUS authentication:
  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name eapol-block mac-radius
  ```

- To configure EAPoL block for a client authenticated using captive portal authentication:
  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name eapol-block captive-portal
  ```

SEE ALSO

- Understanding Authentication on Switches | 361

RELATED DOCUMENTATION

- Access Control and Authentication on Switching Devices | 361
Central Web Authentication

Web authentication provides access to network for users by redirecting the client’s Web browser to a central Web authentication server (CWA server), which handles the complete login process. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Understanding Central Web Authentication

Web authentication redirects Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed access to the network. Web authentication is useful for providing network access to temporary users, such as visitors to a corporate site, who try to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices, but fail authentication because of other issues, such as expired network credentials.

Web authentication can be done locally on the switch using captive portal, but this requires that the Web portal pages be configured on each switch used as a network access device. Central Web authentication (CWA) provides efficiency and scaling benefits by redirecting the client’s Web browser to a central Web authentication server (CWA server), which handles the complete login process.
Central Web Authentication Process

Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The host can attempt authentication using 802.1X authentication first, but must then attempt MAC RADIUS authentication before attempting central Web authentication. The switch, operating as the authenticator, exchanges RADIUS messages with the authentication, authorization, and accounting (AAA) server. After MAC RADIUS authentication fails, the switch receives an Access-Accept message from the AAA server. This message includes a dynamic firewall filter and a redirect URL for central Web authentication. The switch applies the filter, which allows the host to receive an IP address, and uses the URL to redirect the host to the Web authentication page.

The host is prompted for login credentials and might also be asked to agree to an acceptable use policy. If Web authentication is successful, the AAA server sends a Change of Authorization (CoA) message, which updates the terms of the authorized session in progress. This enables the authenticator to update the filter or VLAN assignment applied to the controlled port, to allow the host to access the LAN.

The sequence of events in central Web authentication is as follows (see Figure 20 on page 512):

1. A host connected to the switch (authenticator) initiates MAC RADIUS authentication.

2. MAC RADIUS authentication fails. Instead of sending an Access-Reject message to the switch, the AAA server sends an Access-Accept message that includes a dynamic firewall filter and a CWA redirect URL.

3. The host is allowed by the terms of the filter to send DHCP requests.

4. The host receives an IP address and DNS information from the DHCP server. The AAA server initiates a new session that has a unique session ID.

5. The host opens a Web browser.

6. The authenticator sends the CWA redirect URL to the host.

7. The host is redirected to the CWA server and is prompted for login credentials.

8. The host provides the username and password.

9. After successful Web authentication, the AAA server sends a CoA message to update the filter or VLAN assignment applied on the controlled port, allowing the host to access the LAN.
10. The authenticator responds with a CoA-ACK message and sends a MAC RADIUS authentication request to the AAA server.

11. The AAA server matches the session ID to the appropriate access policy and sends an Access-Accept message to authenticate the host.

Dynamic Firewall Filters for Central Web Authentication

Central Web authentication uses dynamic firewall filters, which are centrally defined on the AAA server and dynamically applied to supplicants that request authentication through that server. The filter allows the host to get an IP address dynamically using DHCP. You define the filters by using RADIUS attributes, which are included in the Access-Accept messages sent from the server. Filters can be defined using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter with the correct terms that allow the destination IP address of the CWA server. This configuration is done directly on the AAA server. To use the Filter-ID attribute for central web authentication, enter the value as JNPR_RSVD_FILTER_CWA on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required. For more information about configuring dynamic firewall filters for central web authentication, see "Configuring Central Web Authentication" on page 513.
Redirect URL for Central Web Authentication

In central Web authentication, the authenticator redirects the host's Web browser request to the CWA server by using a redirect URL. After redirection, the CWA server completes the login process. The redirect URL for central web authentication can be configured on the AAA server or on the authenticator. The redirect URL, along with the dynamic firewall filter, must be present to trigger the central web authentication process after the failure of MAC RADIUS authentication.

The redirect URL can be centrally defined on the AAA server by using the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter. You can also configure the redirect URL locally on the host interface by using the CLI statement `redirect-url` at the `[edit protocols dot1x authenticator interface interface-name]` hierarchy level. For more information about configuring the redirect URL, see “Configuring Central Web Authentication” on page 513.

SEE ALSO

- Understanding Dynamic Filters Based on RADIUS Attributes | 405
- Understanding Dynamic VLAN Assignment Using RADIUS Attributes | 406
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395

Configuring Central Web Authentication

IN THIS SECTION

- Configuring Dynamic Firewall Filters for Central Web Authentication | 514
- Configuring the Redirect URL for Central Web Authentication | 515
- Guidelines for Configuring Central Web Authentication | 516

Central Web authentication is a fallback method of authentication in which the host's Web browser is redirected to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.
Central Web authentication is invoked after a host has failed MAC RADIUS authentication. The switch, operating as the authenticator, receives a RADIUS Access-Accept message from the AAA server that includes a dynamic firewall filter and a redirect URL for central Web authentication. The dynamic firewall filter and the redirect URL must both be present for the central Web authentication process to be triggered.

### Configuring Dynamic Firewall Filters for Central Web Authentication

Dynamic firewall filters are used in central Web authentication to enable the host to get an IP address from a DHCP server, which allows the host to access the network. The filters are defined on the AAA server using RADIUS attributes, which are sent to the authenticator in an Access-Accept message. You can define the filter using either the Juniper-Switching-Filter attribute, which is a vendor-specific attribute (VSA), or the Filter-ID attribute, which is an IETF RADIUS attribute.

- To use the Juniper-Switching-Filter VSA for central Web authentication, you must configure the filter terms directly on the AAA server. The filter must include a term to match the destination IP address of the CWA server with the action `allow`.
  
  For example:

  ```
  001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
  Session-Timeout = "300",
  Juniper-CWA-Redirect-URL = "https://10.10.10.10",
  Juniper-Switching-Filter = "Match Destination-ip 10.10.10.10 Action allow,
  Match ip-protocol 17 Action allow, Match Destination-mac 00:01:02:33:44:55 Action deny"
  ```

  **NOTE:** The switch does not resolve the DNS queries for the redirect URL. You must configure the Juniper-Switching-Filter attribute to allow the destination IP address of the CWA server.

- To use the Filter-ID attribute for central Web authentication, enter `JNPR_RSVD_FILTER_CWA` as the value for the attribute on the AAA server. The filter terms for this attribute are internally defined for central Web authentication, because of which no additional configuration is required.

  For example:

  ```
  001122334455 Auth-Type := EAP, Cleartext-Password :="001122334455"
  Session-Timeout = "300",
  Juniper-CWA-Redirect-URL = "https://10.10.10.10",
  Filter-Id = "JNPR_RSVD_FILTER_CWA",
  ```
For more information about configuring dynamic firewall filters on the AAA server, see the documentation for your AAA server.

**Configuring the Redirect URL for Central Web Authentication**

In central Web authentication, the authenticator redirects the host’s Web browser request to the CWA server by using a redirect URL. The redirect URL for central Web authentication can be configured on the AAA server or locally on the host interface.

- To configure the redirect URL on the AAA server, use the Juniper-CWA-Redirect VSA, which is attribute number 50 in the Juniper RADIUS dictionary. The URL is forwarded from the AAA server to the switch in the same RADIUS Access-Accept message that contains the dynamic firewall filter.

  For example:

  ```
  001122334455 Auth-Type := EAP, Cleartext-Password := "001122334455"
  Session-Timeout = "300",
  Juniper-CWA-Redirect-URL = "https://10.10.10.10",
  Filter-Id = "JNPR_RSVD_FILTER_CWA",
  ```

  **NOTE:** When the special Filter-ID attribute JNPR_RSVD_FILTER_CWA is used for the dynamic firewall filter, the redirect URL must include the IP address of the AAA server, for example, `https://10.10.10.10`.

- To configure the redirect URL locally on the host interface, use the following CLI statement:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface interface-name redirect-url
  ```

  For example:

  ```
  user@switch# show protocols dot1x authenticator 
  authentication-name-profile auth1;
  interface {
    ge-0/0/1.0 {
      supplicant single;
      mac-radius;
      redirect-url https://10.10.10.10;
    }
  }
  ```
Guidelines for Configuring Central Web Authentication

Central Web authentication is triggered after the failure of MAC RADIUS authentication when the redirect URL and dynamic firewall filter are both present. The redirect URL and dynamic firewall filter can be configured in any of the following combinations:

1. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.

2. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the `redirect-url` CLI statement and the dynamic firewall filter is configured on the AAA server by using the Juniper-Switching-Filter VSA. The filter must be configured to allow the destination IP address of the CWA server in this case.

3. The AAA server sends both the CWA redirect URL and dynamic firewall filter to the authenticator. The redirect URL is configured on the AAA server by using the Juniper-CWA-Redirect VSA and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value `JNPR_RSVD_FILTER_CWA`. The redirect URL must contain the IP address of the CWA server in this case.

4. The AAA server sends the dynamic firewall filter to the authenticator and the redirect URL is configured locally on the host port. The redirect URL is configured on the authenticator by using the `redirect-url` CLI statement and the dynamic firewall filter is configured on the AAA server by using the Filter-ID attribute with the value `JNPR_RSVD_FILTER_CWA`. The redirect URL must contain the IP address of the CWA server in this case.

RELATED DOCUMENTATION

- Configuring Central Web Authentication with EX Series Switches and Aruba ClearPass
Centralized Access Control to Network Resources on EX Series Switches

Network access control (NAC) allows you to control access to network resources such as servers, applications, and stored data.

You can use Junos Pulse Access Control Service and the switches for a centralized end-to-end NAC system. The Access Control Service eliminates the need to configure firewall filters on each switch. Instead, you define resource access policies centrally on the NAC device. For more information, read this topic.

Understanding Centralized Network Access Control and EX Series Switches
Network access control (NAC) allows you to control who is admitted to the network and what resources—servers, applications, and stored data—those users are allowed to access. These controls include:

- Authentication—Pre-admission controls
- Authorization—Post-admission controls

You can use different methods to implement NAC on Juniper Networks EX Series Ethernet Switches. This topic describes:

**NAC Using Any RADIUS Server and Access Policies Defined on the Local Switch**

For pre-admission controls, you can use the switch in combination with any RADIUS server as the *authentication server*. For additional information, see "Understanding Authentication on Switches" on page 361.

For post-admission controls, you can configure firewall filters to limit access to specific resources. For additional information, see *Firewall Filters for EX Series Switches Overview*.

**Centralized NAC Using Junos Pulse Access Control Service**

You can use Junos Pulse Access Control Service and the switches for a centralized end-to-end NAC system, including both pre-admission *authentication* and post-admission *authorization*.

When you configure such a system, the Juniper Networks MAG Series Junos Pulse Gateways or the Juniper Networks IC Series Unified Access Control Appliances NAC device functions as the authentication server. For messages relating to IEEE 802.1X and MAC RADIUS authentication, the NAC device communicates with the switch using the RADIUS protocol.

The Access Control Service also performs additional functions. It eliminates the need to configure firewall filters on each switch. Instead, you define resource access policies centrally on the NAC device. This centralized method is particularly helpful when you have multiple switches in your network.

The resource access policy on the Access Control Service defines which network resources are allowed and denied for a user, based upon the user's role. The NAC device distributes these policies to all connected switches. The NAC device thus functions as a centralized policy management server. For messages relating to access policies, the NAC device communicates with the switch using the Junos UAC Enforcer Protocol (JUEP). The switch converts the resource access policies into filter definitions and applies these to the appropriate port.
NOTE: With this solution, the EX Series switch serves as an Intranet Enforcer, that is, a policy enforcement point for the Access Control Service. The Access Control Service sends auth table entries and resource access policies when an endpoint successfully completes 802.1X authentication or MAC authentication (unmanaged devices). Access for any endpoint is governed by the resource access policies that you configure on the Access Control Service. Because resource access policies are employed, firewall filters are not required for the switch configuration.

This integrated solution of Access Control Service and EX Series switches is easier to implement and much more efficient than previous versions of Access Control Service and the switches. As soon the switch connects to the MAG Series or IC Series NAC device, the Access Control Service pushes the role-based policies to the switch via JUEP. This enables the user to access the network more quickly than previous implementations, because the policy is already available on the switch and does not need to be pushed from the centralized device at the time of user authentication. Moreover, the policy push happens only once, which utilizes network bandwidth efficiently and makes this implementation suitable for scaled environments.

If you change policies, the Access Control Service automatically pushes the updated policies to the connected switch. The switch applies the policies dynamically without taking users through another authentication transaction.

NOTE: Do not configure firewall filters on the switch and do not use RADIUS server attributes for firewall filters if you are configuring the switch to use the Access Control Service. Instead, specify or deny access to resources by using the Access Control Service resource access policies.

You create policies on the NAC device’s administrative interface to control access to resources and services. Access is based on successful authentication, the user’s assigned role, and the security compliance of the endpoint device. For example, you can provide full access to protected resources employee role and limited access for a contractor role.

Captive Portal Authentication

Captive portal authentication allows you to authenticate users on the switches by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network. The details of configuring captive portal authentication differ depending on whether you are using the Access Control Service:

- If you have connected the switch to the Access Control Service, use the Access Control Service NAC device as an external captive portal server for redirecting Web browser requests. When users try to access a protected network resource that is connected to the switch, the user must first sign in to the
Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service. When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

See “Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)” on page 523. You can use the same Access Control Service as the external captive portal server for more than one switch.

- If you are not using the Access Control Service, you can use captive portal to redirect users to a login page that you configure on the local switch. See “Designing a Captive Portal Authentication Login Page on Switches” on page 494 for information about designing a login page on your switch.

---

### Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

You can connect the switch to Junos Pulse Access Control Service to set up a centralized, end-to-end network access control (NAC) system, which allows you to control who is admitted to the network and what resources those users are allowed to access.

The Access Control Service functions both as an authentication server (RADIUS server) and as a centralized policy management server.

Before you begin configuring the switch to connect to the Access Control Service:

- Configure a resource access policy.
- Obtain the password of the Access Control Service.
- Obtain the IP address of the Access Control Service.
To configure the switch to work with the Access Control Service:

1. Configure the switch to use the Access Control Service for authentication and authorization:

   ```
   [edit ethernet-switching-options]
   user@switch# set uac-policy
   ```

2. Configure the access profile to specify the Access Control Service. The access profile contains the authentication and authorization configuration that aids in handling authentication and authorization requests, including the authentication method and sequence, and the Access Control Service address:
   a. Configure `radius` as the authentication method to be used when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches:

   ```
   [edit access profile]
   user@switch# set profile-name authentication-order radius
   ```
   b. Specify the IP address of the authentication server:

   ```
   [edit access profile]
   user@switch# set profile-name radius authentication-server ip-address
   ```

3. Configure the RADIUS server to use the same IP address that you specified for the authentication server:

   ```
   [edit access]
   user@switch# set radius-server ip-address
   ```

4. Configure the password to use for connecting the switch with the RADIUS server:

   ```
   [edit access]
   user@switch# set radius-server password
   ```

   **NOTE:** The password specified here is used for RADIUS communications between the switch and the Access Control Service. It does not need to match the password that is specified on the Access Control Service through the administrative interface on the Access Control Service.
[edit access]
user@switch# set radius-server secret password

5. Configure the address of the Access Control Service MAG Series or the IC Series NAC device:

   NOTE: Specify the hostname and IP address of the NAC device. This is the same IP address that you used for specifying the authentication server.

[edit services united-access-control infranet-controller hostname]
user@switch# set address ip-address

6. Configure the switch’s management Ethernet interface for the NAC device:

[edit services united-access-control infranet-controller hostname]
user@switch# set interface me0.0

7. Configure the password for connecting the switch to the Access Control Service NAC device:

   NOTE: This password must match the password specified on the Access Control Service though its administrative interface. It is used for Junos UAC Enforcer Protocol (JUEP) communications between the switch and the Access Control Service.

[edit services united-access-control infranet-controller hostname]
user@switch# set password password

8. Configure the amount of time that switch waits to receive a response from the Access Control Service:

[edit services united-access-control]
user@switch# set timeout seconds

9. Specify the time between continuity-check messages for the switch’s connection with the Access Control Service:

[edit services united-access-control]
user@switch# set interval seconds

10. Specify an action for the switch to take if a timeout occurs for the connection between the switch and the Access Control Service:

[edit services united-access-control]
11. Specify the name of the access profile to use for 802.1X, MAC RADIUS, or captive portal authentication:

```
NOTE: Use the same access profile that you configured previously (step 2).
```

```
[edit protocols dot1x]
user@switch# set authenticator authentication-profile-name profile-name
```

12. Configure the 802.1X interface that the switch will use for communicating with the Access Control Service:

```
[edit protocols dot1x]
user@switch# set authenticator interface interface-name
```

---

**Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)**

If you have connected the EX Series switch to the Junos Pulse Access Control Service and you want to use the captive portal user authentication feature, configure the Access Control Service network access control (NAC) device as an external captive portal server. The captive portal feature is required only for user authentication. Unmanaged devices, such as printers or phones, can be authenticated through 802.1X and MAC address authentication.

When users try to access a protected network resource that is connected to the switch, the user must first sign in to the Access Control Service for authentication and endpoint security checking. The captive portal redirects the user to a login page located on the Access Control Service.

When the sign-in page for the Access Control Service is displayed, the user signs in and the Access Control Service examines the endpoint for compliance with security policies. If the endpoint passes the security check, access is granted to the protected resource.

Before you begin, be sure you have:

- Configured access between the switch and the Access Control Service. See “Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)” on page 520.
- Designed your captive portal login page on the Access Control Service.
To configure the switch to use the Access Control Service for captive portal:

1. Configure captive portal to authenticate clients connected to the switch for access to use the authentication profile that directs the client to the Access Control Service:

   NOTE: The access profile name specified here must match the access profile name that you specified for the Access Control Service in "Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)" on page 520.

   ```
   [edit]
   user@switch# set services captive-portal authentication-profile-name access-profile-name
   ```

2. Enable an interface for use with captive portal authentication:

   ```
   [edit]
   user@switch# set services captive-portal interface interface-name supplicant multiple
   ```

3. (Optional) Specify which clients are to bypass captive portal authentication:

   ```
   [edit]
   user@switch# set ethernet-switching-options authentication-whitelist mac-address
   ```

   NOTE: You can use `set ethernet-switching-options authentication-whitelist mac-address interface interface-name` to limit the scope to the interface.

   NOTE: If the client is already attached to the switch, you must clear its MAC address from captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the authentication whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Central Web Authentication</th>
<th>510</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive Portal Authentication</td>
<td>485</td>
</tr>
</tbody>
</table>
You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. For more information, read this topic.

### Understanding 802.1X and VoIP on EX Series Switches

When you use VoIP, you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls by using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple supplicant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 21 on page 526.
If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single supplicant mode. In single supplicant mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see Figure 22 on page 527.
If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN.

**Multi Domain 802.1X Authentication**

Multi-domain 802.1X authentication is an extension of multiple supplicant mode that allows one default VoIP device and multiple data devices to authenticate on a single port. Multi-domain 802.1X authentication provides enhanced security over multiple supplicant mode by restricting the number of authenticated data and VoIP sessions on the port. In multiple supplicant mode, any number of VoIP or data sessions can be authenticated; the number of sessions can be restricted using MAC limiting, but there is no way to apply the limit specifically to either data or VoIP sessions.

With multi-domain 802.1X authentication, the single port is divided into two domains; one is the data domain and the other is the voice domain. Multi-domain 802.1X authentication maintains separate session counts based on the domain. You can configure the maximum number of authenticated data sessions allowed on the port. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed on the port.

If a new client attempts to authenticate on the interface after the maximum session count has been reached, the default action is to drop the packet and generate an error log message. You can also configure the action to shut down the interface. The port can be manually recovered from the down state by issuing the
clear dot1x recovery-timeout command, or by can recover automatically after a configured recovery timeout period.

Multi-domain authentication does not enforce the order of device authentication. However, for the best results, the VoIP device should be authenticated before a data device on a multi domain 802.1X-enabled port. Multi-domain authentication is supported only in multiple supplicant mode.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 661

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch

IN THIS SECTION

- Requirements | 529
- Overview and Topology | 529
- Configuration | 531
- Verification | 534

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as the LLDP-MED protocol and 802.1X authentication:

NOTE: If your switch runs Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see “Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support” on page 558. For ELS details, see Using the Enhanced Layer 2 Software CLI.
Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya 9620 IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See Installing and Connecting an EX3200 Switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (J-Web Procedure).
- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see Configuring PoE on EX Series Switches (CLI Procedure).

NOTE: If the IP address isn’t configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the voip statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN’s ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4200 switch is connected to an Avaya 9620 IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so
the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on interface **ge-0/0/10** (see Figure 23 on page 530).

**Figure 23: VoIP Topology**

In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

**Table 34 on page 531** describes the components used in this VoIP configuration example.
Table 34: Components of the VoIP Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 switch</td>
</tr>
<tr>
<td>VLAN names</td>
<td>data-vlan</td>
</tr>
<tr>
<td></td>
<td>voice-vlan</td>
</tr>
<tr>
<td>Connection to Avaya phone—with integrated hub, to connect</td>
<td>ge-0/0/2</td>
</tr>
<tr>
<td>phone and desktop PC to a single interface (requires PoE)</td>
<td></td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Provides backend database connected to the</td>
</tr>
<tr>
<td></td>
<td>switch through interface ge-0/0/10.</td>
</tr>
</tbody>
</table>

As well as configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to multiple supplicant to support more than one supplicant’s access to the LAN through interface ge-0/0/2.

- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

NOTE: A PoE configuration is not necessary if an IP telephone is using a power adapter.

Configuration

To configure VoIP, LLDP-MED, and 802.1X authentication:

CLI Quick Configuration

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple

Step-by-Step Procedure
To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99

2. Associate the VLAN data-vlan with the interface:

   [edit vlans]
   user@switch# set data-vlan interface ge-0/0/2.0

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the data-vlan VLAN:

   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access

4. Configure VoIP on the interface and specify the assured-forwarding forwarding class to provide the most dependable class of service:

   [edit ethernet-switching-options]
   user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
   user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding

5. Configure LLDP-MED protocol support:

   [edit protocols]
   user@switch# set lldp-med interface ge-0/0/2.0

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify multiple supplicant mode:
NOTE: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple

Results
Display the results of the configuration:

[edit]
user@switch# show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}

protocols {
  lldp-med {
    interface ge-0/0/2.0;
  }
  dot1x {
    authenticator {
      interface {
        ge-0/0/2.0 {
          supplicant multiple;
        }
      }
    }
  }
}

vlans {
  data-vlan {
    vlan-id 77;
  }
}
To confirm that the configuration is working properly, perform these tasks:

**Verifying LLDP-MED Configuration**

**Purpose**
Verify that LLDP-MED is enabled on the interface.

**Action**

```
user@switch> show lldp detail
```

LLDP          : Enabled
Advertisement interval : 30 Second(s)
Transmit delay          : 2 Second(s)
Hold timer : 2 Second(s)
Config Trap Interval : 300 Second(s)
Connection Hold timer : 60 Second(s)

LLDP MED : Enabled
MED fast start count : 3 Packet(s)

<table>
<thead>
<tr>
<th>Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Neighbor count</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enabled</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>-</td>
<td>Enabled</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>VLAN-id</th>
<th>VLAN-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>0</td>
<td>default</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>0</td>
<td>data-vlan</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>99</td>
<td>voice-vlan</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>0</td>
<td>default</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>20</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>0</td>
<td>default</td>
</tr>
</tbody>
</table>

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System
description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port
VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power
Via MDI.

Meaning
The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2.0` interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose
Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

**Action**

```
user@switch> show dot1x interface ge/0/0/2.0 detail
```

```
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

**Meaning**

The field **Role** shows that the **ge-0/0/2.0** interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

**Verifying the VLAN Association with the Interface**

**Purpose**

Display the interface state and VLAN membership.

**Action**

```
user@switch> show ethernet-switching interfaces
```
Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>up</td>
<td>voice-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data-vlan</td>
<td>unblocked</td>
</tr>
</tbody>
</table>

**Meaning**

The field **VLAN members** shows that the **ge-0/0/2.0** interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN. The **State** field shows that the interface is up.

**SEE ALSO**

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Defining CoS Forwarding Classes (CLI Procedure)
- Defining CoS Forwarding Classes (J-Web Procedure)
- Configuring LLDP-MED (CLI Procedure) | 665

**Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support**

**IN THIS SECTION**

- Requirements | 538
- Overview | 538
You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

**Requirements**

This example uses the following hardware and software components:

- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 13.2X50 or later for EX Series switches.

Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support*.
- Configured the IP phone as a member of the voice VLAN.
- *(Optional)* Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE on EX Series Switches (CLI Procedure)*.

**Overview**

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept
untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see “Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support” on page 558.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the switch is connected to a non-LLDP-MED IP phone.

NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

CLI Quick Configuration
To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
```
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding

Step-by-Step Procedure

1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

**NOTE:** The voice VLAN ID must be set manually on the IP phone.

2. Associate the VLAN data-vlan with the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan switch-options interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member data-vlan
```

4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

5. Specify the assured-forwarding forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

Results

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
```
family ethernet-switching {
  port-mode access;
  vlan {
    members data-vlan;
  }
}
}
}
}
}
vlans {
  data-vlan {
    vlan-id 77;
    interface {
      ge-0/0/2.0;
    }
  }
  voice-vlan {
    vlan-id 99;
  }
}
}
edgethernet-switching options {
  voip {
    interface ge-0/0/2.0 {
      vlan voice-vlan;
      forwarding-class assured-forwarding;
    }
  }
}
}

Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

CLI Quick Configuration
To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

[edit]

set vlans data-vlan vlan-id 77

set vlans voice-vlan vlan-id 99

set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan

set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
**Step-by-Step Procedure**

1. Configure two VLANs: one for data traffic and one for voice traffic:

   ```
   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99
   ```

   **NOTE:** The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
   ```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
   ```

**Results**

Display the results of the configuration:

```
[edit]
user@switch> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members voice-vlan;
        }
        native-vlan-id data-vlan;
      }
    }
  }
  vlans {
    data-vlan {
```
Verification

IN THIS SECTION

- Verifying the VLAN Association With the Interface | 543

To confirm that the configuration is working properly, perform the following task:

**Verifying the VLAN Association With the Interface**

**Purpose**
Display the interface state and VLAN membership.

**Action**

```
user@switch> show ethernet-switching interfaces
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>up</td>
<td>voice-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data-vlan</td>
<td>unblocked</td>
</tr>
</tbody>
</table>
Meaning

The field VLAN members shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The State field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 661

Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support

IN THIS SECTION

- Requirements | 544
- Overview | 545
- Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port | 546
- Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option | 548
- Verification | 549

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol is sometimes used with IP phones to forward VoIP parameters from the switch to the phone. However, not all IP phones support LLDP-MED.

This example describes how to configure VoIP on an EX Series switch without using LLDP-MED:

Requirements

This example uses the following hardware and software components:

- One EX4200 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An IP phone that does not support LLDP-MED.
- Junos OS Release 9.1 or later for EX Series switches.
Before you configure VoIP, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.

- Configured the IP phone as a member of the voice VLAN.

- (Optional) Configured interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. See *Configuring PoE on EX Series Switches (CLI Procedure)*.

**Overview**

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You can also power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

EX Series switches can accommodate an IP telephone and end host connected to a single switch port. In such a scenario, voice and data traffic must be separated into different broadcast domains, or VLANs. One method for accomplishing this is by configuring a voice VLAN, which enables access ports to accept untagged data traffic as well as tagged voice traffic from IP phones, and associate each type of traffic with separate and distinct VLANs. Voice traffic (tagged) can then be treated differently, generally with a higher priority than data traffic (untagged).

The voice VLAN delivers the greatest benefit when used with IP phones that support LLDP-MED, but it is flexible enough that IP phones that do not support LLDP-MED can also use it effectively. However, in the absence of LLDP-MED, the voice VLAN ID must be set manually on the IP phone because LLDP-MED is not available to accomplish this dynamically. For information about setting up a voice VLAN for IP phones that support LLDP-MED, see “Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch” on page 528.

Another method to separate voice (tagged) and data (untagged) traffic into different VLANs is to use a trunk port with the native VLAN ID option. The trunk port is added as a member of the voice VLAN, and processes only tagged voice traffic from that VLAN. The trunk port must also be configured with the native VLAN ID for the data VLAN so that it can process untagged data traffic from the data VLAN. This configuration also requires that the voice VLAN ID be set manually on the IP phone.

This example illustrates both methods. In this example, the interface ge-0/0/2 on the EX4200 switch is connected to a non-LLDP-MED IP phone.
NOTE: The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

Configuring VoIP Without LLDP-MED by Using a Voice VLAN on an Access Port

CLI Quick Configuration
To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
```

Step-by-Step Procedure
1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

NOTE: The voice VLAN ID must be set manually on the IP phone.

2. Configure the VLAN data-vlan on the interface ge-0/0/2:

```
[edit vlans]
user@switch# set data-vlan interface ge-0/0/2.0
```

3. Configure the interface ge-0/0/2 as an access port belonging to the data VLAN:
4. Configure VoIP on the interface ge-0/0/2 and add this interface to the voice VLAN:

```bash
[edit ethernet-switching-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
```

Results

Display the results of the configuration:

```bash
[edit]
user@switch> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}
}
vans {
  data-vlan {
    vlan-id 77;
    interface {
      ge-0/0/2.0;
    }
  }
  voice-vlan {
    vlan-id 99;
  }
}
}
ethernet-switching options {
  voip {
    interface ge-0/0/2.0 {
      vlan voice-vlan;
    }
  }
}
```
Configuring VoIP Without LLDP-MED by Using a Trunk Port with Native VLAN Option

CLI Quick Configuration
To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members voice-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Step-by-Step Procedure
1. Configure two VLANs: one for data traffic and one for voice traffic:

```
[edit vlans]
user@switch# set data-vlan vlan-id 77
user@switch# set voice-vlan vlan-id 99
```

**NOTE:** The voice VLAN ID must be set manually on the IP phone.

2. Configure interface ge-0/0/2 as a trunk port that includes only the voice VLAN:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan member voice-vlan
```

3. Configure the native VLAN ID for the data VLAN on the trunk port:

```
[edit interfaces]
user@switch# set ge-0/0/2 unit 0 family ethernet-switching native-vlan-id data-vlan
```

Results
Display the results of the configuration:

```plaintext
[edit]
user@switch> show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members voice-vlan;
          }
          native-vlan-id data-vlan;
        }
      }
    }
  }
}
vlans {
  data-vlan {
    vlan-id 77;
  }
  voice-vlan {
    vlan-id 99;
  }
}
```

Verification

**IN THIS SECTION**

- Verifying the VLAN Association With the Interface | 549

To confirm that the configuration is working properly, perform the following task:

**Verifying the VLAN Association With the Interface**

**Purpose**

Display the interface state and VLAN membership.
Action

```
user@switch> show ethernet-switching interfaces

Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces
Interface   State    VLAN members           Blocking
ge-0/0/0.0  down     default                unblocked
ge-0/0/1.0  down     employee-vlan          unblocked
ge-0/0/5.0  down     employee-vlan          unblocked
ge-0/0/3.0  down     employee-vlan          unblocked
ge-0/0/8.0  down     employee-vlan          unblocked
ge-0/0/10.0 down     default                unblocked
ge-0/0/11.0 down     employee-vlan          unblocked
ge-0/0/23.0 down     default                unblocked
ge-0/0/2.0  up       voice-vlan             unblocked
data-vlan             unblocked
```

Meaning

The field VLAN members shows that the ge-0/0/2.0 interface supports both the data VLAN, data-vlan, and the voice VLAN, voice-vlan. The State field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 661

Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication

IN THIS SECTION

- Requirements | 551
- Overview | 552
- Configuration | 552
- Verification | 555
You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication using static MAC bypass of authentication:

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- An IP telephone

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*.
- Configured the RADIUS server for 802.1X authentication and set up the access profile. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 400.
- (Optional) Configured interface `ge-0/0/2` for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see *Configuring PoE on EX Series Switches (CLI Procedure)*.

NOTE: If the IP address isn't configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the `voip` statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN’s ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).
Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4200 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

To configure VoIP without 802.1X authentication:

CLI Quick Configuration

To quickly configure VoIP, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching port-mode access
set ethernet-switching-options voip interface ge-0/0/2.0 vlan voice-vlan
set ethernet-switching-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2.0
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Step-by-Step Procedure
To configure VoIP without 802.1X:

1. Configure the VLANs for voice and data:

   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99

2. Associate the VLAN data-vlan with the interface:

   [edit vlans]
   user@switch# set data-vlan interface ge-0/0/2.0

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the data-vlan VLAN:

   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching port-mode access

4. Configure VoIP on the interface and specify the assured-forwarding forwarding class to provide the most dependable class of service:

   [edit ethernet-switching-options]
   user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
   user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding

5. Configure LLDP-MED protocol support:

   [edit protocols]
   user@switch# set lldp-med interface ge-0/0/2.0

6. Set the authentication profile (see "Configuring 802.1X Interface Settings (CLI Procedure)" on page 390 and "Configuring 802.1X RADIUS Accounting (CLI Procedure)" on page 438):

   [edit protocols]
   set dot1x authenticator authentication-profile-name auth-profile

7. Add the MAC address of the phone to the static MAC bypass list:

   [edit protocols]
   set dot1x authenticator static 00:04:f2:11:aa:a7

8. Set the supplicant mode to multiple:

   [edit protocols]
set dot1x authenticator interface ge-0/0/2.0 supplicant multiple

Results
Display the results of the configuration:

[edit]
user@switch# show configuration
interfaces {
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                port-mode access;
                vlan {
                    members data-vlan;
                }
            }
        }
    }
}

protocols {
    lldp-med {
        interface ge-0/0/2.0;
    }
    dot1x {
        authenticator {
            authentication-profile-name auth-profile;
            static {
                00:04:f2:11:aa:a7;
            }
        }
        interface {
            ge-0/0/2.0 {
                supplicant multiple;
            }
        }
    }
}

vlans {
    data-vlan {
        vlan-id 77;
        interface {
            ge-0/0/2.0;
        }
    }
}
voice-vlan {
  vlan-id 99;
}
}
ethernet-switching options {
  voip {
    interface ge-0/0/2.0 {
      vlan voice-vlan;
      forwarding-class assured-forwarding;
    }
    }
    }
}

Verification

IN THIS SECTION
- Verifying LLDP-MED Configuration | 555
- Verifying Authentication for the Desktop PC | 556
- Verifying the VLAN Association with the Interface | 557

To confirm that the configuration is working properly, perform these tasks:

**Verifying LLDP-MED Configuration**

**Purpose**
Verify that LLDP-MED is enabled on the interface.

**Action**

```
user@switch> show lldp detail
```

<table>
<thead>
<tr>
<th>LLDP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement interval</td>
<td>30 Second(s)</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>2 Second(s)</td>
</tr>
<tr>
<td>Hold timer</td>
<td>2 Second(s)</td>
</tr>
<tr>
<td>Config Trap Interval</td>
<td>300 Second(s)</td>
</tr>
<tr>
<td>Connection Hold timer</td>
<td>60 Second(s)</td>
</tr>
</tbody>
</table>
LLDP MED : Enabled
MED fast start count : 3 Packet(s)

<table>
<thead>
<tr>
<th>Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Neighbor count</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enabled</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>-</td>
<td>Enabled</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>VLAN-id</th>
<th>VLAN-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>0</td>
<td>default</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>0</td>
<td>data-vlan</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>99</td>
<td>voice-vlan</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>0</td>
<td>default</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>0</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>0</td>
<td>default</td>
</tr>
</tbody>
</table>

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

LLDP 802 TLVs supported:
Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

LLDP MED TLVs supported:
LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

**Meaning**

The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2.0` interface. The end of the output shows the list of supported LLDP basic TLVs, 802.3 TLVs, and LLDP-MED TLVs that are supported.

**Verifying Authentication for the Desktop PC**

**Purpose**

Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.
**Action**

user@switch> **show dot1x interface ge/0/0.2 detail**

```
ge-0/0/2.0
   Role: Authenticator
   Administrative state: Auto
   Supplicant mode: Multiple
   Number of retries: 3
   Quiet period: 60 seconds
   Transmit period: 30 seconds
   Mac Radius: Disabled
   Mac Radius Restrict: Disabled
   Reauthentication: Enabled
   Configured Reauthentication interval: 3600 seconds
   Supplicant timeout: 30 seconds
   Server timeout: 30 seconds
   Maximum EAPOL requests: 2
   Guest VLAN member: <not configured>
   Number of connected supplicants: 1
   Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

**Meaning**

The field **Role** shows that the **ge-0/0.2.0** interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

**Verifying the VLAN Association with the Interface**

**Purpose**

Display the interface state and VLAN membership.

**Action**

user@switch> **show ethernet-switching interfaces**
Ethernet-switching table: 0 entries, 0 learned

user@switch> show ethernet-switching interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>up</td>
<td>voice-vlan</td>
<td>unblocked</td>
</tr>
</tbody>
</table>

Meaning
The field VLAN members shows that the ge-0/0/2.0 interface supports both the data-vlan VLAN and voice-vlan VLAN. The State field shows that the interface is up.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 661

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support

IN THIS SECTION
- Requirements | 559
- Overview and Topology | 560
- Configuration | 562
- Verification | 565
NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see “Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch” on page 528. For ELS details, see Using the Enhanced Layer 2 Software CLI.

You can configure VoIP on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as how to configure the LLDP-MED protocol and 802.1X authentication:

Requirements

This example uses the following software and hardware components:

NOTE: This example also applies to QFX5100 switches.

- Junos OS Release 13.2X50 or later for EX Series switches
- One EX Series switch with support for ELS acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).
- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch with ELS Support or Example: Setting Up Basic Bridging and a VLAN on Switches.
• Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 400.

• (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant uses a power adapter. For information about configuring PoE, see Configuring PoE on EX Series Switches (CLI Procedure).

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the voip statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX Series switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that enables you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see Figure 24 on page 561).

NOTE: This figure also applies to QFX5100 switches.
In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

**Table 35 on page 561** describes the components used in this VoIP configuration example.

### Table 35: Components of the VoIP Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX Series switch with support for ELS.</td>
</tr>
</tbody>
</table>
Table 35: Components of the VoIP Configuration Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
</table>
| VLAN names and IDs | data-vlan, 77  
voice-vlan, 99 |
| Connection to Avaya phone—with integrated hub, to connect phone and desktop PC to a single interface (requires PoE) | ge-0/0/2 |
| One RADIUS server | Provides backend database connected to the switch through interface ge-0/0/10 |

Besides configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to **multiple** supplicant mode to support more than one supplicant's access to the LAN through interface ge-0/0/2.

- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

  **NOTE:** A PoE configuration is not necessary if an IP telephone uses a power adapter.

**Configuration**

**CLI Quick Configuration**
To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
```
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan

set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding

set protocols lldp-med interface ge-0/0/2

set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple

Step-by-Step Procedure
To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99

2. Associate the VLAN data-vlan with the interface:

   [edit vlans]
   user@switch# set data-vlan switch-options interface ge-0/0/2.0

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the interface as a member of the data-vlan VLAN:

   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan

4. Configure VoIP on the interface and specify the assured-forwarding forwarding class to provide the most dependable class of service:

   [edit switch-options]
   user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
   user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding

5. Configure LLDP-MED protocol support:

   [edit protocols]
   user@switch# set lldp-med interface ge-0/0/2

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify multiple supplicant mode:
NOTE: If you do not want to authenticate any device, skip the 802.1X configuration on this interface.

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

Results
Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces {
  ge-0/0/2 {
    unit 0 {
      family ethernet-switching {
        interface-mode access;
        vlan {
          members data-vlan;
        }
      }
    }
  }
}
protocols {
  lldp-med {
    interface ge-0/0/2;
  }
  dot1x {
    authenticator {
      interface {
        ge-0/0/2.0 {
          supplicant multiple;
        }
      }
    }
  }
}
vlans {
  data-vlan {
    vlan-id 77;
  }
}
```
Verification

IN THIS SECTION
- Verifying LLDP-MED Configuration | 565
- Verifying 802.1X Authentication for IP Phone and Desktop PC | 567
- Verifying the VLAN Association with the Interface | 567

To confirm that the configuration is working properly, perform these tasks:

Verifying LLDP-MED Configuration

Purpose
Verify that LLDP-MED is enabled on the interface.

Action

user@switch> show lldp detail

LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Enabled
MED fast start count : 3 Packets

Port ID TLV subtype : locally-assigned

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Power Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>all</td>
<td>-</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>-</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td>-</td>
<td>Enabled</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td>77</td>
<td>vlan-77</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
</tbody>
</table>

Basic Management TLVs supported:
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name, System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size, Port VLAN tag, Port VLAN name.

Meaning
The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2` interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.
Verifying 802.1X Authentication for IP Phone and Desktop PC

Purpose
Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.

Action

```
user@switch> show dot1x interface ge/0/0/2.0 detail
```

```
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user101, 00:04:0f:fd:ac:fe
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: vo11
      Dynamic Filter: match source-dot1q-tag 10 action deny
      Session Reauth interval: 60 seconds
      Reauthentication due in 50 seconds
```

Meaning
The field Role shows that the ge-0/0/2.0 interface is in the authenticator state. The Supplicant mode field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

Verifying the VLAN Association with the Interface

Purpose
Display the interface's VLAN membership.
Action

user@switch> show ethernet-switching interface ge-0/0/2.0

Routing Instance Name: default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
LH - MAC limit hit, DN - interface down)

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Vlan members</th>
<th>TAG limit</th>
<th>STP state</th>
<th>Logical interface flags</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/2.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>untagged</td>
</tr>
<tr>
<td>voice-vlan 99</td>
<td></td>
<td>65535</td>
<td>Discarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data-vlan 77</td>
<td></td>
<td>65535</td>
<td>Discarding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Meaning
The field VLAN members shows that the ge-0/0/2.0 interface supports both the data-vlan VLAN and voice-vlan VLAN.

SEE ALSO
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Defining CoS Forwarding Classes (CLI Procedure)
- Defining CoS Forwarding Classes (J-Web Procedure)
- Configuring LLDP-MED (CLI Procedure) | 665

RELATED DOCUMENTATION
- RADIUS Server Configuration for Authentication | 378
- 802.1X Authentication | 386
Configuring IEEE 802.1x Port-Based Network Access Control

IEEE 802.1x Port-Based Network Access Control Overview | 571
Understanding the Administrative State of the Authenticator Port | 572
Understanding the Administrative Mode of the Authenticator Port | 572
Configuring the Authenticator | 573
Viewing the dot1x Configuration | 574
IEEE 802.1x Port-Based Network Access Control Overview

MX Series routers support the IEEE 802.1x Port-Based Network Access Control (dot1x) protocol on Ethernet interfaces for validation of client and user credentials to prevent unauthorized access to a specified router port. Before authentication is complete, only 802.1x control packets are allowed and forwarded to the router control plane for processing. All other packets are dropped.

Authentication methods used must be 802.1x compliant. Authentication using RADIUS and Microsoft Active Directory servers is supported. The following user/client authentication methods are allowed:

- EAP-MD5 (RFC 3748)
- EAP-TTLS requires a server certificate (RFC 2716)
- EAP-TLS requires a client and server certificate
- PEAP requires only a server certificate

You can use both client and server certificates in all types of authentication except EAP-MD5.

NOTE: On the MX Series router, 802.1x can be enabled on bridged ports only and not on routed ports.

Dynamic changes to a user session are supported to allow the router administrator to terminate an already authenticated session by using the "RADIUS disconnect" message defined in RFC 3576.

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the Administrative State of the Authenticator Port</td>
<td>572</td>
</tr>
<tr>
<td>Understanding the Administrative Mode of the Authenticator Port</td>
<td>572</td>
</tr>
<tr>
<td>Configuring the Authenticator</td>
<td>573</td>
</tr>
<tr>
<td>Viewing the dot1x Configuration</td>
<td>574</td>
</tr>
<tr>
<td>Ethernet Interfaces Feature Guide for Routing Devices</td>
<td></td>
</tr>
</tbody>
</table>
Understanding the Administrative State of the Authenticator Port

The administrative state of an authenticator port can take any of the following three states:

- **Force authorized**—Allows network access to all users of the port without requiring them to be authenticated. This is equivalent to not having any authentication enabled on the port.

- **Force unauthorized**—Denies network access to all users of the port. This is equivalent to disabling the port.

- **Automatic**—This is the default mode where the authentication server response determines if the port is opened for traffic or not. Only the successfully authenticated clients are allowed access, all others are denied.

In Junos OS, the default mode is "automatic." The "force authorized" and "force unauthorized" admin modes are not supported. You can achieve the functionality of "force authorized" mode by disabling `dot1x` on the required port. You can achieve the functionality of "force unauthorized" mode by disabling the port itself.

Related Documentation:

- IEEE 802.1x Port-Based Network Access Control Overview | 571
- Understanding the Administrative Mode of the Authenticator Port | 572
- Configuring the Authenticator | 573
- Viewing the dot1x Configuration | 574
- Ethernet Interfaces Feature Guide for Routing Devices

Understanding the Administrative Mode of the Authenticator Port

Junos OS supports the supplicant mode “single” and not the “single secure” nor “multiple” modes. The "Single" mode option authenticates only the first client that connects to a port. All other clients that connect later (802.1x compliant or noncompliant) are allowed free access on that port without any further
authentication. If the first authenticated client logs out, all other users are locked out until a client authenticates again.

RELATED DOCUMENTATION

IEEE 802.1x Port-Based Network Access Control Overview | 571
Understanding the Administrative State of the Authenticator Port | 572
Configuring the Authenticator | 573
Viewing the dot1x Configuration | 574

Ethernet Interfaces Feature Guide for Routing Devices

Configuring the Authenticator

To configure the IEEE 802.1x Port-Based Network Access Control protocol on Ethernet interfaces you must configure the `authenticator` statement at the `[edit protocols dot1x]` hierarchy level. Use the `authentication-profile-name access-profile-name` statement to specify the authenticating RADIUS server, and use the `interface` statement to specify and configure the Gigabit Ethernet or Fast Ethernet interface on the router specifically for IEEE 802.1x protocol use; both at the `[edit protocols dot1x authenticator]` hierarchy level.

```
[edit protocols dot1x]
authenticator {
    authentication-profile-name access-profile-name;
    interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) {
        maximum-requests seconds;
        quiet-period seconds;
        reauthentication (disable | interval seconds);
        retries integer;
        server-timeout seconds;
        supplicant (single);
        supplicant-timeout seconds;
        transmit-period seconds;
    }
}
```
Viewing the dot1x Configuration

**Purpose**
To review and verify the dot1x configuration.

**Action**
To view all dot1x configurations, use the `show dot1x interface` operational mode command. To view a dot1x configuration for a specific interface, use the `show dot1x interface (xe-fpc/pic/port | ge-fpc/pic/port | fe-fpc/pic/port) detail` operational mode command. See the Network Interfaces Command Reference for more information about this command.
# Configuring IEEE 802.1x Port-Based Network Access Control in Enhanced LAN Mode

802.1X for MX Series Routers in Enhanced LAN Mode Overview | 577

Understanding 802.1X and LLDP and LLDP-MED on MX Series Routers in Enhanced LAN Mode | 581

Understanding 802.1X and RADIUS Accounting on MX Series Routers in Enhanced LAN Mode | 584

Understanding 802.1X and VoIP on MX Series Routers in Enhanced LAN Mode | 585

Understanding Guest VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode | 588

Understanding Dynamic VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode | 588

Understanding Server Fail Fallback and Authentication on MX Series Routers in Enhanced LAN Mode | 589

Configuring 802.1X RADIUS Accounting on MX Series Routers in Enhanced LAN Mode | 590
Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode | 593

Configuring LLDP-MED on MX Series Routers in Enhanced LAN Mode | 595

Configuring LLDP on MX Series Routers in Enhanced LAN Mode | 597

Configuring Server Fail Fallback on MX Series Routers in Enhanced LAN Mode | 601

Understanding Captive Portal Authentication on the MX Series Routers | 603

Understanding Authentication Session Timeout on MX Series Routers | 604

Authentication Process Flow for MX Series Routers in Enhanced LAN Mode | 605

Specifying RADIUS Server Connections on an MX Series Router in Enhanced LAN Mode | 607

Configuring Captive Portal Authentication on MX Series Routers in Enhanced LAN Mode | 608

Designing a Captive Portal Authentication Login Page on an MX Series Router | 611

Configuring Static MAC Bypass of Authentication on MX Series Routers in Enhanced LAN Mode | 614

Controlling Authentication Session Timeouts on an MX Series Router in Enhanced LAN Mode | 615

Configuring MAC RADIUS Authentication on MX Series Routers in Enhanced LAN Mode | 617

Example: Configuring MAC RADIUS Authentication on an MX Series Router | 619

Example: Setting Up Captive Portal Authentication on an MX Series Router | 624

Example: Connecting a RADIUS Server for 802.1X to an MX Series Router | 631

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an MX Series Router | 635

Example: Configuring Static MAC Bypass of Authentication on an MX Series Router | 639

Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on MX Series Routers | 644
802.1X for MX Series Routers in Enhanced LAN Mode
Overview
Starting with Junos OS Release 14.2, IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. Support is implemented for controlling access to your network through an MX Series router by using several different authentication methods, such as 802.1X, MAC RADIUS, or a captive portal.

This functionality is supported on the following MPCs on MX240, MX480, and MX960 routers in enhanced LAN mode:

- MPC4E with two 100-Gigabit Ethernet ports and eight 10-Gigabit Ethernet ports
- MPC4E with thirty-two 10-Gigabit Ethernet ports
- MPC3E that contains a 2-port 40-Gigabit Ethernet MIC with QSFP+
- MPC1E with forty 1-Gigabit Ethernet ports or twenty 1-Gigabit Ethernet ports

You must reboot the router when you configure or delete the enhanced LAN mode on the router. Configuring the `network-services lan` option implies that the system is running in the enhanced IP mode. When you configure a device to function in MX-LAN mode, only the supported configuration statements and operational show commands that are available for enabling or viewing in this mode are displayed in the CLI interface. If your system contains parameters that are not supported in MX-LAN mode in a configuration file, you cannot commit those unsupported attributes. You must remove the settings that are not supported and then commit the configuration. After the successful CLI commit, a system reboot is required for the attributes to be come effective. Similarly, if you remove the `network-services lan` statement, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. If your configuration file contains settings that are supported only in MX-LAN mode, you must remove those attributes before you commit the configuration. After the successful CLI commit, a system reboot will be required for the CLI settings to take effect. The Layer 2 Next-Generation CLI configuration settings are supported in MX-LAN mode. As a result, the typical MX Series-format of CLI configurations might differ in MX-LAN mode.

This functionality is supported on an MX Series Virtual Chassis combination that functions in enhanced LAN mode (by entering the `network-services lan` statement at the [edit chassis] hierarchy level). Port-based network access control is supported on MX240, MX480, and MX960 routers with MPCs in both the MX-LAN mode and the non-MX-LAN mode (with other supported network services modes on MPCs on these routers). To configure the IEEE 802.1x port-based network access control (PNAC) protocol on Ethernet interfaces, you must configure the `authenticator` statement at the [edit protocols authentication-access-control] hierarchy level. You can also configure captive portal authentication on a router so that users connected to the switch are authenticated before being allowed to access the network. You can also configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources by using the `uac-policy` statement.
How 802.1X Authentication Works

802.1X authentication works by using an Authenticator Port Access Entity (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant’s credentials are presented and matched on the Authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in either single mode, single-secure mode, or multiple mode:

- **single**—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the end devices’ authentication.

- **single-secure**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.

- **multiple**—Allows multiple end devices to connect to the port. Each end device will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

- Whether or not the end device is 802.1X-enabled.
- Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.
- Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See “Configuring RADIUS Server Fail Fallback (CLI Procedure)” on page 384.
802.1X Features Overview

NOTE: The 802.1X features available on the MX Series routers depend upon which switch you are using.

802.1X features on Juniper Networks MX Series routers are:

- Guest VLAN—Provides limited access to a LAN, typically just to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access just to the Internet and to other guests' end devices.
- Server-reject VLAN—Provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.
- Server-fail VLAN—Provides limited access to a LAN, typically just to the Internet, for 802.1X end devices during a RADIUS server timeout.
- Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.
- Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).
- Dynamic changes to a user session—Allows the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

Supported Features Related to 802.1X Authentication

802.1X does not replace other security technologies. 802.1X works together with port security features, such as DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting, to guard against spoofing.

Supported features related to authentication include:

- Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.
• MAC RADIUS authentication—Provides a means to enable or disable MAC authentication independently of whether 802.1X authentication is enabled.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access. Support is implemented for controlling access to your network through an MX Series router by using several different authentication methods, such as 802.1X, MAC RADIUS, or a captive portal.</td>
</tr>
</tbody>
</table>

Understanding 802.1X and LLDP and LLDP-MED on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, Juniper Networks MX Series routers use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the router to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Juniper Networks Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the router and the IP telephone.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the router to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the router interface to which it connects.

The router also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

EX Series routers support the following basic TLVs:
- **Chassis Identifier**—The MAC address associated with the local system.

  NOTE: The Chassis ID TLV has a subtype for Network Address Family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

- **Port Identifier**—The port identification for the specified port in the local system.

- **Port Description**—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV will contain the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit, so only the description configured on the physical interface can be used.

- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.

- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.

- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.

- **Management Address**—The IPv4 or IPv6 management address of the local system.

EX Series routers support the following 802.3 TLVs:

- **Power via MDI**—A TLV that advertises MDI power support, PSE power pair, and power class information.

- **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is not configurable, but based on the physical interface structure.

  NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field will contain a value of other or unknown if the LLDP packet was transmitted from a 10-gigabit SFP+ port.

- **Link Aggregation**—A TLV that advertises if the port is aggregated and its aggregated port ID.

- **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.

- **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.
EX Series routers support the following LLDP-MED TLVs:

- **LLDP MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
  - 0—Capabilities
  - 1—Network Policy
  - 2—Location Identification
  - 3—Extended Power via MDI-PSE
  - 4—Inventory
  - 5–15—Reserved

- **LLDP-MED Device Class Values**:
  - 0—Class not defined.
  - 1—Class 1 Device.
  - 2—Class 2 Device.
  - 3—Class 3 Device.
  - 4—Network Connectivity Device
  - 5–255—Reserved.

- **Network Policy**—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.

- **Endpoint Location**—A TLV that advertises the physical location of the endpoint.

- **Extended Power via MDI**—A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, Juniper Networks MX Series routers use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the router to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.</td>
</tr>
</tbody>
</table>
Understanding 802.1X and RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

Juniper Networks MX Series routers support IETF RFC 2866, RADIUS Accounting. Starting with Junos OS Release 14.2, you can configure RADIUS accounting on an MX Series router which enables statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. In the event that the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Juniper Networks Junos operating system (Junos OS).

The RADIUS accounting process between a switch and a RADIUS server works like this:

1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. The switch forwards an accounting-request packet containing an event record to the accounting server. For example, a supplicant is authenticated through 802.1X authentication and connected to the LAN. The event record associated with this supplicant contains an Acct-Status-Type attribute whose value indicates the beginning of user service for this supplicant. When the supplicant’s session ends, the accounting request will contain an Acct-Status-Type attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.

3. The RADIUS accounting server logs these events as start-accounting or stop-accounting records. The records are in a file. On FreeRADIUS, the file name is the server’s address; for example, 122.69.1.250.

4. The accounting server sends an accounting-response packet back to the switch confirming it has received the accounting request.

5. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.
Starting with Junos OS Release 14.2, you can configure RADIUS accounting on an MX Series router which enables statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

Understanding 802.1X and VoIP on MX Series Routers in Enhanced LAN Mode

When you use Voice over IP (VoIP), you can connect IP telephones to the router and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. Starting with Junos OS Release 14.2, 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In multiple-suppliant mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 21 on page 526.
If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single-suppliant mode. In single-suppliant mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see Figure 22 on page 527.
If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN.

**Release History Table**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.</td>
</tr>
</tbody>
</table>
Understanding Guest VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled
- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants sending incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet</td>
</tr>
</tbody>
</table>

Understanding Dynamic VLANs for 802.1X on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.

When this feature is configured on the RADIUS server, an end device or user authenticating on the RADIUS server is assigned to the VLAN configured for it. The end device or user becomes a member of a VLAN
dynamically after successful 802.1X authentication. For information on configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

Successful authentication requires that the VLAN ID or VLAN name exist on the router and match the VLAN ID or VLAN name sent by the RADIUS server during authentication. If neither exists, the end device is unauthenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.</td>
</tr>
</tbody>
</table>

Understanding Server Fail Fallback and Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Juniper Networks MX Series routers in enhanced LAN mode use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication are configured on the interface, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the MX Series router opens the interface to permit access.

A RADIUS server timeout occurs if no RADIUS authentication servers are reachable when an end device logs in and attempts to access the LAN. Server fail fallback allows you to specify one of four actions to be taken toward end devices awaiting authentication when the server is timed out:

- **Permit** authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- **Deny** authentication, preventing traffic from flowing from the end device through the interface. This is the default.
• Move the end device to a specified VLAN. (The VLAN must already exist on the router.)

• Sustain authenticated end devices that already have LAN access and deny unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device’s first attempt at authentication through the RADIUS server.

Server fail fallback allows you to specify that an end device be moved to a specified VLAN if the router receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.</td>
</tr>
</tbody>
</table>

Configuring 802.1X RADIUS Accounting on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure basic RADIUS accounting using the CLI:

1. Specify the accounting servers to which the switch will forward accounting statistics:

   ```
   [edit access]
   user@router# set profile profile1 radius accounting-server accounting-server [122.69.1.250 122.69.1.252]
   ```

2. Define the RADIUS accounting servers:

   ```
   [edit access]
   user@router# set radius-server 122.69.1.250 secret juniper
   ```
user@router# set radius-server 122.69.1.252 secret juniper1

3. Enable accounting for an access profile:

[edit access]
user@router# set profile profile1 accounting

4. Configure the RADIUS servers to use while sending accounting messages and updates:

[edit access]
user@router# set profile profile1 accounting order radius

5. Configure the statistics to be collected on the router and forwarded to the accounting server:

[edit access ]
user@router# set profile profile1 accounting accounting-stop-on-access-deny
user@router# set profile profile1 accounting accounting-stop-on-failure

6. Display accounting statistics collected on the router:

user@router> show network-access aaa statistics accounting

Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timeout: 0

7. Open an accounting log on the RADIUS accounting server using the server's address, and view accounting statistics:

[root@freeradius]# cd /usr/local/var/log/radius/radacct/122.69.1.250
[root@freeradius 122.69.1.250]# ls

  detail-20071214

[root@freeradius 122.69.1.250]# vi details-20071214

  User-Name = "000347e1bab9"
  NAS-Port = 67
  Acct-Status-Type = Stop
  Acct-Session-Id = "802.1x811912"
Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION
Configuring 802.1X Interface Settings on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant’s credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:

• You can also specify an 802.1X exclusion list to specify supplicants can that can bypass authentication and be automatically connected to the LAN.

• You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

• You cannot configure 802.1X user authentication on redundant trunk groups (RTGs).

Before you begin, specify the RADIUS server or servers to be used as the authentication server.

To configure 802.1X on an interface:

1. Configure the supplicant mode as single (authenticates the first supplicant), single-secure (authenticates only one supplicant), or multiple (authenticates multiple supplicants):

   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5 supplicant multiple

2. Enable reauthentication and specify the reauthentication interval:

   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5/0 dot1x reauthentication interval 5

3. Configure the interface timeout value for the response from the supplicant:

   [edit protocols authentication-access-control]
   user@switch# set interface ge-0/0/5 dot1x supplicant-timeout 5

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

   [edit protocols authentication-access-control]
user@switch#  set interface ge-0/0/5 server-timeout 5

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

   [edit protocols authentication-access-control]
   user@switch#  set interface ge-0/0/5 dot1x transmit-period 60

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

   [edit protocols authentication-access-control]
   user@switch#  set interface ge-0/0/5 dot1x maximum-requests 5

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

   [edit protocols authentication-access-control]
   user@switch#  set interface ge-0/0/5 retries 1

**NOTE:** This setting specifies the number of tries before the switch puts the interface in a “HELD” state.

---

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant’s credentials are presented and matched on the authentication server (a RADIUS server).</td>
</tr>
</tbody>
</table>

---

**RELATED DOCUMENTATION**
Configuring LLDP-MED on MX Series Routers in Enhanced LAN Mode

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. Starting with Junos OS Release 14.2, the router uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is turned on by default on MX Series routers.

This topic describes:

- Enabling LLDP-MED on Interfaces | 595
- Configuring Location Information Advertised by the Router | 595
- Configuring for Fast Start | 596

### Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@router# set interface (LLDP-MED) ge-0/0/2.0
```

### Configuring Location Information Advertised by the Router

You can configure the location information that is advertised from the router to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

```
[edit protocols lldp-med]
user@router# set interface ge-0/0/2.0 location civic-based country-code US
user@router# set interface ge-0/0/2.0 location civic-based ca-type 1 ca-value "El Dorado County"
user@router# set interface ge-0/0/2.0 location civic-based ca-type 2 ca-value CA
```
user@router# set interface ge-0/0/2.0 location civic-based ca-type 3 ca-value Somerset
user@router# set interface ge-0/0/2.0 location civic-based ca-type 6 ca-value "Mount Aukum Road"
user@router# set interface ge-0/0/2.0 location civic-based ca-type 19 ca-value 6450
user@router# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value "Holiday Market"

• To specify a location using an elin string:

    [edit protocols lldp-med]
    user@router# set interface ge-0/0/2.0 location elin 4085551212

---

### Configuring for Fast Start

You can specify the number of LLDP-MED advertisements sent from the router in the first second after it has detected an LLDP-MED device. The default is 3; to set it to another value:

    [edit protocols lldp-med]
    user@router# set fast-start 6

---

**NOTE:** If an interface is configured as a VoIP interface, then the router does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

---

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, the router uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.</td>
</tr>
</tbody>
</table>

---

**RELATED DOCUMENTATION**
Configuring LLDP on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

- Enabling LLDP on Interfaces | 597
- Adjusting LLDP Advertisement Settings | 598
- Adjusting SNMP Notification Settings of LLDP Changes | 599
- Specifying a Management Address for the LLDP Management TLV | 600

Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

  [edit protocols lldp]
  user@router# set interface all

- To configure LLDP on a specific interface:

  [edit protocols lldp]
  user@router# set interface interface-name

**NOTE:** On MX Series routers, LLDP cannot be configured on the management Ethernet interface. Issuing the command set protocols lldp interfaceem0 generates the following error message:

```
error: name: 'em0': Invalid interface
error: statement creation failed: interface
```
Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

  ```
  [edit protocols lldp]
  user@router# set advertisement-interval seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@router# set advertisement-interval 45
  ```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the advertisement-interval value):

  ```
  [edit protocols lldp]
  user@router# set hold-multiplier seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@router# set hold-multiplier 5
  ```

- To specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the advertisement-interval value is set to 8 seconds or more) or 1 second (if the advertisement-interval value is set to less than 8 seconds).

  ```
  [edit protocols lldp]
  user@router# set transmit-delay seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set transmit-delay 2
  ```
NOTE: The *advertisement-interval* value must be greater than or equal to four times the *transmit-delay* value; otherwise, an error is returned when you attempt to commit the configuration.

### Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to 0, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

  ```
  [edit protocols lldp]
  user@router# set lldp-configuration-notification-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set lldp-configuration-notification-interval 600
  ```

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-trap-interval seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-trap-interval 600
  ```

- To specify the holding time (used in combination with the *ptopo-configuration-trap-interval* value) to maintain dynamic topology entries (in seconds):

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-maximum-hold-time seconds
  ```

  For example:

  ```
  [edit protocols lldp]
  user@router# set ptopo-configuration-maximum-hold-time 2147483647
  ```
Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only out-of-band management addresses must be used as the value for the `management-address` statement.

To configure the management address:

```
[edit protocols lldp]
user@router# set management-address ip-address
```

**NOTE:** Ensure that the interface with the configured management address has LLDP enabled using the `set protocols lldp interface` command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the `show lldp local-information` command output will not display the correct interface information.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links.</td>
</tr>
</tbody>
</table>
Configuring Server Fail Fallback on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an authenticator port access entity (the router) to block all traffic to and from an end device at the interface until the end device’s credentials are presented and matched on the authentication server (a RADIUS server). When the end device has been authenticated, the router stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the router, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the router and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the router does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. Server fail fallback allows you to configure authentication alternatives that permit the router to take appropriate actions toward end devices awaiting authentication or reauthentication.

NOTE: The authentication fallback method called server-reject VLAN provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.
To configure basic server fail fallback options using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

  ```
  [edit protocols authentication-access-control]
  user@router# set interface ge-0/0/1 dot1x server-fail permit
  ```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

  ```
  [edit protocols authentication-access-control]
  user@router# set interface ge-0/0/1 dot1x server-fail deny
  ```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs (in this case, the VLAN name is `vlan1`):

  ```
  [edit protocols authentication-access-control]
  user@router# set interface ge-0/0/1 dot1x server-fail vlan-name vlan1
  ```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

  ```
  [edit protocols authentication-access-control]
  user@router# set interface ge-0/0/1 dot1x server-fail use-cache
  ```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the router (in this case, the VLAN name is `vlan-sf`):

  ```
  [edit protocols authentication-access-control]
  user@router# set interface ge-0/0/1 dot1x server-reject-vlan vlan-sf
  ```

**NOTE:** If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, server fail fallback allows you to specify how end devices connected to the router are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.</td>
</tr>
</tbody>
</table>
Understanding Captive Portal Authentication on the MX Series Routers

Starting with Junos OS Release 14.2, captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on MX Series routers by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos Software for MX Series routers provides a template that allows you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time a client connected to a captive portal interface attempts to access a webpage, the switch presents the captive portal login page. Upon successful authentication, the user is allowed access to the network and to continue to the original page requested.

NOTE: If Hypertext Transfer Protocol Secure (HTTPS) is enabled, Hypertext Transfer Protocol (HTTP) requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the client is returned to the HTTP connection.

If there are clients that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC address to an authentication whitelist. (If the MAC address has already been learned on the interface, you must clear it using the `clear captive-portal interface interface-name`) before adding it to the whitelist.)

When the user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Limitations of Captive Portal

Captive portal on MX Series routers has the following limitations:

- The captive portal interface must be configured for **family ethernet-switching** and set to port mode access. The VLAN must be configured with a routed VLAN interface (RVI).
- The DHCP gateway IP address for the switch must be configured as the IP address of the routed VLAN interface.
- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.
- If the user is idle for more than about 5 minutes and there is no traffic passed, the user is required to log back in to the captive portal.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on MX Series routers by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network.</td>
</tr>
</tbody>
</table>

### Understanding Authentication Session Timeout on MX Series Routers

Starting with Junos OS Release 14.2, you can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

For captive portal authentication, the length of the session depends on the value configured for the `session-expiry` statement. The remainder of this topic pertains only to 802.1X and MAC RADIUS authentication sessions.

For 802.1X and MAC RADIUS authentication sessions, the timeout of the session depends on the value of `reauthentication-interval` for `dot1x authentication`. The authentication session might also end when the MAC table aging time expires because, unless you configure it not to, the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table.

Information about each 802.1X and MAC RADIUS authentication session—including the associated interfaces and VLANs for each MAC address that is authenticated by 802.1X authentication or MAC RADIUS authentication—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured `mac-table-aging-time` value, the switch removes the MAC address from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication database, with the result that the session ends.
You can control variables affecting timeout of authentication sessions in the following ways:

- Set the authentication session timeout on all interfaces or on selected interfaces using the `reauthentication` statement.
- Disassociate the authentication session table from the Ethernet switching table using the `no-mac-table-binding` statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.</td>
</tr>
</tbody>
</table>

### Authentication Process Flow for MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can control access to your network through an MX Series router by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

**Figure 6 on page 369** illustrates the authentication process:
Figure 27: Authentication Process Flow for an MX Series Router

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can control access to your network through an MX Series router by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.</td>
</tr>
</tbody>
</table>
Specifying RADIUS Server Connections on an MX Series Router in Enhanced LAN Mode

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant's credentials or MAC address are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the router stops blocking access and opens the interface to the supplicant.

Starting with Junos OS Release 14.2, to use 802.1X or MAC RADIUS authentication, you must specify the connections on the router for each RADIUS server to which you will connect.

To configure a RADIUS server on the router:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the router must match the secret password on the server:

   ```
   [edit access]
   user@router# set radius-server 10.0.0.100 port 1812 secret abc
   ```

   **NOTE:** Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the router is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the router.

   ```
   [edit access]
   user@router# set radius-server source-address 10.93.14.100
   ```

3. Configure the authentication order, making radius the first method of authentication:

   ```
   [edit access]
   user@router# set profile profile1 authentication-order radius
   ```
4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers.

```
[edit access profile]
user@router# set atlanta radius authentication-server 10.0.0.100 10.2.14.200
```

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

```
[edit access profile]
user@router# set protocols authentication-access-control authentication-profile-name denver
```

6. Configure the IP address of the MX Series router in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, to use 802.1X or MAC RADIUS authentication, you must specify the connections on the router for each RADIUS server to which you will connect.</td>
</tr>
</tbody>
</table>

## Configuring Captive Portal Authentication on MX Series Routers in Enhanced LAN Mode

**NOTE:** This example uses Junos OS for MX240, MX480, and MX960 routers with support for the Enhanced LAN mode configuration style. If your router does not run MX-LAN mode, you cannot configure port-based authentication settings in the same manner as described in this section. If you remove the network-services lan statement in the [edit chassis] hierarchy level, the system does not run in MX-LAN mode. Therefore, all of the settings that are supported outside of the MX-LAN mode are displayed and are available for definition in the CLI interface. In such a scenario, you must use the statements at the [edit protocols dot1x] hierarchy level to configure 802.1x and MAC RADIUS authentication, and the options at the [edit services captive-portal] hierarchy level to configure captive portal authentication. In MX-LAN mode, you can configure all the port-based network access control methodologies using the statements at the [edit protocols authentication-access-control] hierarchy level.
Starting with Junos OS Release 14.2, configure captive portal authentication (hereafter referred to as captive portal) on an MX Series router so that users connected to the router are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal
- Enabling an Interface for Captive Portal
- Configuring Bypass of Captive Portal Authentication

---

### Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the router:

   ```
   [edit]
   user@router# set system services web-management https local-certificate my-signed-cert
   ```

   **NOTE:** You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@router# set protocols custom-options-captive-portal secure-authentication https
   ```

---
Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@router# set authentication-access-control interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@router# set authentication-access-control static 00:10:12:e0:28:22
```

**NOTE:** Optionally, you can use `set authentication-access-control static 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

**NOTE:** If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address session-mac-addr` command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, configure captive portal authentication (hereafter referred to as captive portal) on an MX Series router so that users connected to the router are authenticated before being allowed to access the network.</td>
</tr>
</tbody>
</table>
Designing a Captive Portal Authentication Login Page on an MX Series Router

Starting with Junos OS Release 14.2, you can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access. Upon successful authentication, the user is allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the "Terms and Conditions of Use". By clicking the Agree button, the user can access the captive portal login page.

Figure 19 on page 495 shows an example of a captive portal login page:

Figure 28: Example of a Captive Portal Login Page

Table 33 on page 495 summarizes the configurable elements of a captive portal login page.
Table 36: Configurable Elements of a Captive Portal Login Page

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footer background color</td>
<td>footer-bgcolor hex-color</td>
<td>The HTML hexadecimal code for the background color of the captive portal login page footer.</td>
</tr>
<tr>
<td>Footer message</td>
<td>footer-message text-string</td>
<td>Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy. The default text shown in the footer is Copyright @2010, Juniper Networks Inc.</td>
</tr>
<tr>
<td>Footer text color</td>
<td>footer-text-color color</td>
<td>Color of the text in the footer. The default color is white.</td>
</tr>
<tr>
<td>Form header background color</td>
<td>form-header-bgcolor hex-color</td>
<td>The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.</td>
</tr>
<tr>
<td>Form header message</td>
<td>form-header-message text-string</td>
<td>Text displayed in the header of the captive portal login page. The default text is Captive Portal User Authentication</td>
</tr>
<tr>
<td>Form header text color</td>
<td>form-header-text-color color</td>
<td>Color of the text in the form header. The default color is black.</td>
</tr>
<tr>
<td>Form reset button label</td>
<td>form-reset-label label-name</td>
<td>Using the Reset button, the user can clear the username and password fields on the form.</td>
</tr>
<tr>
<td>Form submit button label</td>
<td>form-submit-label label-name</td>
<td>Using the Login button, the user can submit the login information.</td>
</tr>
<tr>
<td>Header background color</td>
<td>header-bgcolor hex-color</td>
<td>The HTML hexadecimal code for the background color of the captive portal login page header.</td>
</tr>
<tr>
<td>Header logo</td>
<td>header-logo filename</td>
<td>Filename of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format. You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.</td>
</tr>
<tr>
<td>Header message</td>
<td>header-message text-string</td>
<td>Text displayed in the page header. The default text is User Authentication.</td>
</tr>
</tbody>
</table>
Table 36: Configurable Elements of a Captive Portal Login Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header text color</td>
<td>header-text-color color</td>
<td>Color of the text in the header. The default color is white.</td>
</tr>
<tr>
<td>Post-authentication URL</td>
<td>post-authentication-url</td>
<td>URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.</td>
</tr>
</tbody>
</table>

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:

   ```
   user@router> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
   ```

2. Configure the custom options to specify the background colors and text displayed in the captive portal page:

   ```
   [edit protocols]
   user@router# set captive-portal-custom-options header-bgcolor #006600
   set captive-portal-custom-options header-message "Welcome to Our Network"
   set captive-portal-custom-options banner-message "Please enter your username and password". The banner displays the message "XXXXXXX" by default. The user can modify this message.
   set custom-options footer-message “Copyright ©2010, Our Network”
   ```

Now you can commit the configuration.

**NOTE:** For the custom options that you do not specify, the default value is used.

**Release History Table**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access.</td>
</tr>
</tbody>
</table>
Configuring Static MAC Bypass of Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

  ```
  [edit protocols authentication-access-control]
  user@router# set static 00:04:0f:fd:ac:fe
  ```

- Configure a supplicant to bypass authentication if connected through a particular interface:

  ```
  [edit protocols authentication-access-control]
  user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5
  ```

- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

  ```
  [edit protocols authentication-access-control]
  user@router# set static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment default-vlan
  ```

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.</td>
</tr>
</tbody>
</table>
Controlling Authentication Session Timeouts on an MX Series Router in Enhanced LAN Mode

Starting with Junos OS Release 14.2, for 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the `reauthentication` statement.

The session might also end when the MAC table aging time expires, because the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table. In order to prevent the session from being removed from the authentication session table, you must disassociate the authentication table from the Ethernet switching table using the `no-mac-table-binding` statement.

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server.
- Configure 802.1X authentication on the router.
To configure the authentication session time on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control interface all dot1x reauthentication seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@router# set protocols authentication-access-control interface interface-name dot1x reauthentication seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding on all interfaces:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface all;
```

To remove the binding on a single interface:

```
[edit]
user@router# set protocols authentication-access-control no-mac-table-binding interface interface-name;
```

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, for 802.1X and MAC RADIUS authentication sessions, you can specify authentication session timeout values using the <code>reauthentication</code> statement.</td>
</tr>
</tbody>
</table>

**RELATED DOCUMENTATION**
Configuring MAC RADIUS Authentication on MX Series Routers in Enhanced LAN Mode

Starting with Junos OS Release 14.2, you can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the MX Series router interfaces to which the hosts are connected.

**NOTE:** You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the router first sends the host three EAPOL requests to the host. If there is no response from the host, the router sends the host’s MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the router that the MAC address is a permitted address, and the router opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the `mac-radius restrict` option), the router attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the MX Series router and the RADIUS server.
- Configured MX240, MX480, and MX960 routers to function in enhanced LAN mode by entering the `network-services lan` statement at the `[edit chassis]` hierarchy level.
To configure MAC RADIUS authentication using the CLI:

- On the router, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the restrict qualifier for interface ge-0/0/20 to have it use only MAC RADIUS authentication:

  [edit]
  user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius
  user@router# set protocols authentication-access-control interface ge-0/0/20 dot1x mac-radius restrict

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f):

  [root@freeradius]#
  edit /etc/raddb
  vi users
  00040ffdacfe Auth-type:=Local, User-Password = "00040ffdacfe"
  0004aecd235f Auth-type:=Local, User-Password = "0004aecd235f"

**Release History Table**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the MX Series router interfaces to which the hosts are connected.</td>
</tr>
</tbody>
</table>

**RELATED DOCUMENTATION**
Example: Configuring MAC RADIUS Authentication on an MX Series Router

Starting with Junos OS Release 14.2 to permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the router interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the router will attempt to authenticate the host with the RADIUS server using the host’s MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- An MX Series router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.
Overview and Topology

IEEE 802.1X Port-Based Network Access Control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the router using the 802.1X protocol (are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the router consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the router opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is only connected to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication using the `mac-radius restrict` option, and thus avoid the delay that occurs while the router determines that the device is does not respond to EAP messages.

Two printers are connected to an MX Series router over interfaces, ge-0/0/19 and ge-0/0/20.

Table 27 on page 430 shows the components in the example for MAC RADIUS authentication.

Table 37: Components of the MAC RADIUS Authentication Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router hardware</td>
<td>Ports (ge-0/0/0 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>sales</td>
</tr>
<tr>
<td>Connections to printers</td>
<td>ge-0/0/19, MAC address 00040ffdacfe</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/20, MAC address 0004aecd235f</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>Connected to the router on interface ge-0/0/10</td>
</tr>
</tbody>
</table>

The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the router, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the router attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the `mac radius restrict` option.

Configuration

CLI Quick Configuration
To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius
set protocols authentication-access-control authenticator interface ge-0/0/20 dot1x mac-radius restrict
```

**NOTE:** You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

---

**Step-by-Step Procedure**

Configure MAC RADIUS authentication on the router and on the RADIUS server:

1. On the router, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the *restrict* option on interface ge-0/0/20, so that only MAC RADIUS authentication is used:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/19 dot1x mac-radius
user@router# set protocols authentication-access-control authenticator interface ge-0/0/20 dot1x mac-radius restrict
```

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

```
[root@freeradius]#
edit /etc/raddb
vi users
00040ffdacfe Auth-type:=EAP, User-Password = "00040ffdacfe"
0004aecd235f Auth-type:=EAP, User-Password = "0004aecd235f"
```

**Results**

Display the results of the configuration on the router:

```
user@router> show configuration
protocols {
  authentication-access-control {
    authentication-profile-name profile52;
    interface {
```
Verification

IN THIS SECTION

- Verifying That the Supplicants Are Authenticated | 622

Verify that the supplicants are authenticated:

Verifying That the Supplicants Are Authenticated

Purpose
After supplicants are configured for MAC RADIUS authentication on the router and on the RADIUS server, verify that they are authenticated and display the method of authentication:

Action
Display information about 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

```
user@router> show dot1x interface ge-0/0/19.0 detail
```
ge-0/0/19.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
  Supplicant: user101, 00:04:0f:fd:ac:fe
    Operational state: Authenticated
    Authentication method: Radius
    Authenticated VLAN: vo11
    Dynamic Filter: match source-dot1q-tag 10 action deny
    Session Reauth interval: 60 seconds
    Reauthentication due in 50 seconds

user@router> show dot1x interface ge-0/0/20.0 detail

ge-0/0/20.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Enabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
  Supplicant: user102, 00:04:ae:cd:23:5f
    Operational state: Authenticated
Meaning
The sample output from the show dot1x interface detail command displays the MAC address of the connected end device in the Supplicant field. On interface ge-0/0/19, the MAC address is 00:04:0f:fd:ac:fe, which is the MAC address of the first printer configured for MAC RADIUS authentication. The Authentication method field displays the authentication method as MAC Radius. On interface ge-0/0/20, the MAC address is 00:04:ae:cd:23:5f, which is the MAC address of the second printer configured for MAC RADIUS authentication. The Authentication method field displays the authentication method as MAC Radius.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2 to permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the router interfaces to which the non-802.1X-enabled hosts are connected.</td>
</tr>
</tbody>
</table>

Example: Setting Up Captive Portal Authentication on an MX Series Router
Starting with Junos OS Release 14.2, you can set up captive portal authentication (hereafter referred to as captive portal) on a router to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

This example describes how to set up captive portal on an MX Series router:

### Requirements

This example uses the following hardware and software components:

- An MX Series router that supports captive portal
- Junos OS Release 14.2 or later for MX Series routers

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the router.
- Generated an SSL certificate and installed it on the router.
- Configured basic access between the MX Series router and the RADIUS server.
- Designed your captive portal login page.

### Overview and Topology

This example shows the configuration required on the router to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN without going through captive portal, add its MAC address to the authentication whitelist. The MAC addresses in this list are permitted access on the interface without captive portal.

The topology for this example consists of one MX Series router connected to a RADIUS authentication server. One interface on the router is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

### Configuration

To configure captive portal on your router:

**CLI Quick Configuration**
To quickly configure captive portal on the router after completing the tasks in the Requirements section, copy the following commands and paste them into the router terminal window:

```
[edit]
set system services web-management http
set system services web-management https local-certificate my-signed-cert
set protocols captive-portal-custom-options secure-authentication https
set protocols authentication-access-control interface ge-0/0/10.0 supplicant multiple
set protocols authentication-access-control static 00:10:12:e0:28:22
```

**Step-by-Step Procedure**

To configure captive portal on the router:

1. Enable HTTP access on the router:

```
[edit]
user@router# set system services web-management http
```

2. To create a secure channel for Web access to the router, configure captive portal for HTTPS:

   **NOTE:** You can enable HTTP without enabling HTTPS, but we recommend HTTPS for security purposes.

   a. Associate the security certificate with the Web server and enable HTTPS access on the router:

   ```
   [edit]
   user@router# set system services web-management https local-certificate my-signed-cert
   ```

   b. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@router# set protocols captive-portal-custom-options secure-authentication https
   ```

3. Enable an interface for captive portal:

```
[edit]
user@router# set protocols authentication-access-control interface ge-0/0/10.0 supplicant multiple
```

4. (Optional) Allow specific clients to bypass captive portal:
NOTE: If the client is already attached to the router, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address mac-address` command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address will not be added to the Ethernet routering table and authentication bypass will not be allowed.

```
[edit]
user@router# set protocols authentication-access-control static 00:10:12:e0:28:22
```

NOTE: Optionally, you can use `set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

5. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

```
[edit services captive-portal]
user@router# set protocols captive-portal-custom-options post-authentication-url http://www.my-home-page.com
```

Results
Display the results of the configuration:

```
[edit]
user@router> show
system {
   services {
      web-management {
         http;
         https {
            local-certificate my-signed-cert;
         }
      }
   }
}
security {
   certificates {
      local {
```
Verification

IN THIS SECTION

- Verifying That Captive Portal Is Enabled on the Interface | 628
- Verify That Captive Portal Is Working Correctly | 629

To confirm that captive portal is configured and working properly, perform these tasks:

**Verifying That Captive Portal Is Enabled on the Interface**

**Purpose**
Verify that captive portal is configured on interface ge-0/0/10.
Action

Use the operational mode command `show captive-portal interface interface-name detail`:

```
user@router> show captive-portal interface ge-0/0/10.0 detail
```

<table>
<thead>
<tr>
<th>ge-0/0/10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant mode: Multiple</td>
</tr>
<tr>
<td>Number of retries: 3</td>
</tr>
<tr>
<td>Quiet period: 60 seconds</td>
</tr>
<tr>
<td>Configured CP session timeout: 3600 seconds</td>
</tr>
<tr>
<td>Server timeout: 15 seconds</td>
</tr>
</tbody>
</table>

Meaning

The output confirms that captive portal is configured on interface ge-0/0/10 with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose

Verify that captive portal is working on the router.

Action

Connect a client to interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting

In this section

- Troubleshooting Captive Portal | 630

To troubleshoot captive portal, perform these tasks:
Troubleshooting Captive Portal

Problem
The router does not return the captive portal login page when a user connected to a captive portal interface on the router requests a Web page.

Solution
You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, check the router interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the router.

user@router> show captive-portal firewall ge-0/0/10.0

ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
  Name                          Bytes              Packets
  dot1x_ge-0/0/10_CP_arp         7616                  119
  dot1x_ge-0/0/10_CP_dhcp           0                    0
  dot1x_ge-0/0/10_CP_http           0                    0
  dot1x_ge-0/0/10_CP_https          0                    0
  dot1x_ge-0/0/10_CP_t_dns          0                    0
  dot1x_ge-0/0/10_CP_u_dns          0                    0

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can set up captive portal authentication (hereafter referred to as captive portal) on a router to redirect Web browser requests to a login page that requires the user to input a username and password.</td>
</tr>
</tbody>
</table>
Example: Connecting a RADIUS Server for 802.1X to an MX Series Router

802.1X is the IEEE standard for Port-Based Network Access Control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. Starting with Junos OS Release 14.2, you can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an MX Series router, and configure it for 802.1X:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode and Junos OS Release 14.2R3 for all other routers.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
• Configured users on the RADIUS authentication server.

Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 38: Components of the Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router hardware</td>
<td>MX Series router</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, connect the RADIUS server to access port ge-0/0/10 on the MX Series router. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the MX Series router and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

Configuration

CLI Quick Configuration

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]

set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
```
set access profile profile1 authentication-order radius

set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]

Step-by-Step Procedure

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:

   [edit]
   user@switch# set access radius-server 10.0.0.100 secret juniper
   user@switch# set access radius-server 10.0.0.200 secret juniper

2. Configure the authentication order, making radius the first method of authentication:

   [edit]
   user@switch# set access profile profile1 authentication-order radius

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:

   [edit]
   user@switch# set access profile profile1 radius authentication-server [10.0.0.100 10.0.0.200]

Results

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {
  10.0.0.100
    port 1812;
    secret "$9$qPT3ApBSrv69rvWLVb.P5"; ## SECRET-DATA
  }
} profile profile1{
  authentication-order radius;
  radius {
    authentication-server 10.0.0.100 10.0.0.200;
  }
} }
```
Verification

IN THIS SECTION

- Verify That the Switch and RADIUS Server are Properly Connected

To confirm that the configuration is working properly, perform these tasks:

### Verify That the Switch and RADIUS Server are Properly Connected

#### Purpose
Verify that the RADIUS server is connected to the switch on the specified port.

#### Action
Ping the RADIUS server to verify the connection between the switch and the server:

```bash
user@switch> ping 10.0.0.100

PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

#### Meaning
ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether it is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, you can use a RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.</td>
</tr>
</tbody>
</table>
Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an MX Series Router

Starting with Junos OS Release 14.2, 802.1X on MX Series routers provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as guests, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.
Overview and Topology

The MX Series router acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

Table 39: Components of the Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router hardware</td>
<td>MX Series router</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, access interface ge-0/0/1 provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

Configuration of a Guest VLAN That Includes 802.1X Authentication

CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans bridge-domain-name vlan-id 300
set protocols dot1x authenticator interface all guest-bridge-domain bridge-domain-name
```

Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on MX Series routers:

1. Configure the VLAN ID for the guest VLAN:
[edit]
user@switch# set bridge-domains bridge-domain-name vlan-id 300

2. Configure the guest VLAN under dot1x protocols:

[edit]
user@switch# set protocols dot1x authenticator interface all guest-bridge-domain bridge-domain-name

Results
Check the results of the configuration:

user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-bridge-domain {
            bridge-domain-name;
          }
        }
      }
    }
  }
}
bridge-domains {
  bridge-domain-name {
    vlan-id 300;
  }
}

Verification

IN THIS SECTION
- Verifying That the Guest VLAN is Configured  |  638
To confirm that the configuration is working properly, perform these tasks:

**Verifying That the Guest VLAN is Configured**

**Purpose**
Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.

**Action**
Use the operational mode commands:

```
user@switch> show bridge-domain
```

```
<table>
<thead>
<tr>
<th>Instance</th>
<th>Bridging Domain</th>
<th>Type</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Primary Table</td>
<td></td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>vsl</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>vs1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>vsl</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>guest-vlan</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>vs1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan_dyn</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>
```

```
user@switch> show dot1x interface ge-0/0/1.0 detail
```

ge-0/0/1.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: guest-vlan
Number of connected supplicants: 1
Supplicant: user1, 00:00:00:00:13:23
  Operational state: Authenticated
  Authentication method: Radius
  Authenticated VLAN: vo11
  Dynamic Filter: match source-dot1q-tag 10 action deny
  Session Reauth interval: 60 seconds
  Reauthentication due in 50 seconds

Meaning
The output from the `show bridge domain` command shows bridge-domain-name as the name of the VLAN and the VLAN ID as 300.

The output from the `show dot1x interface ge-0/0/1.0 detail` command displays the bridge domain name, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the bridge-domain-name.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, 802.1X on MX Series routers provides LAN access to users who do not have credentials in the RADIUS database.</td>
</tr>
</tbody>
</table>

Example: Configuring Static MAC Bypass of Authentication on an MX Series Router
Starting with Junos OS Release 14.2, to allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the MX Series router. The static MAC bypass list, also known as the exclusion list, specifies MAC addresses that are allowed on the router without a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host’s MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX240, MX480, or MX960 routers running in enhanced LAN mode.
- One router acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you connect the server to the router, be sure you have:

- Configured enhanced LAN mode on the router.
- Performed basic bridging and VLAN configuration on the router.
- Configured users on the RADIUS authentication server.

### Overview and Topology

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

Consider an MX Series router that functions as an authenticator port. It is connected using the interface, ge-0/0/10, over the IP network to a RADIUS server. The router is also linked to a conference room using the interface, ge-0/0/1, to a printer using the interface, ge-0/0/20, to a hub using the interface, ge-0/0/8, and to two supplicants or clients over interfaces, ge-0/0/2 and ge-0/0/9 respectively.

The interfaces shown in Table 32 on page 482 will be configured for static MAC authentication.
Table 40: Components of the Static MAC Authentication Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router hardware</td>
<td>MX Series router</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>Connections to integrated printer/fax/copier machines (no PoE required)</td>
<td>ge-0/0/19, MAC address 00:04:0f:fd:ac:fe ge-0/0/20, MAC address 00:04:ae:cd:23:5f</td>
</tr>
</tbody>
</table>

The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface ge-0/0/19. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface ge-0/0/20. Both printers will be added to the static list and bypass 802.1X authentication.

Configuration

CLI Quick Configuration
To quickly configure static MAC authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols authentication-access-control interface all supplicant multiple
set protocols authentication-access-control authentication-profile-name profile1
```

Step-by-Step Procedure
Configure static MAC authentication:

1. Configure MAC addresses 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f as static MAC addresses:

   ```
   [edit protocols]
   user@router# set authentication-access-control static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
   ```

2. Configure the 802.1X authentication method:

   ```
   [edit protocols]
   user@router# set authentication-access-control interface all supplicant multiple
   ```

3. Configure the authentication profile name (access profile name) to use for authentication:

   ```
   [edit protocols]
   user@router# set authentication-access-control authentication-profile-name profile1
   ```
Results
Display the results of the configuration:

```
user@router> show
interfaces {
  ge-0/0/19 {
    unit 0 {
      family bridge {
        vlan-id 10;
      }
    }
  }
  ge-0/0/20 {
    unit 0 {
      family bridge {
        vlan-id 10;
      }
    }
  }
}
protocols {
  authentication-access-control {
    authentication-profile-name profile1;
    static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
    interface {
      all {
        supplicant multiple;
      }
    }
  }
}
```
Verification

To confirm that the configuration is working properly, perform these tasks:

Verifying Static MAC Bypass of Authentication

Purpose
Verify that the MAC address for both printers is configured and associated with the correct interfaces.

Action
Use the operational mode command:

```
user@switch> show dot1x static-mac-address
```

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:0f:fd:ac:fe</td>
<td>default</td>
<td>ge-0/0/19.0</td>
</tr>
<tr>
<td>00:04:ae:cd:23:5f</td>
<td>default</td>
<td>ge-0/0/20.0</td>
</tr>
</tbody>
</table>

Meaning
The output field **MAC address** shows the MAC addresses of the two printers.

The output field **Interface** shows that the MAC address **00:04:0f:fd:ac:fe** can connect to the LAN through interface **ge-0/0/19.0** and that the MAC address **00:04:ae:cd:23:5f** can connect to the LAN through interface **ge-0/0/20.0**.

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, to allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the MX Series router.</td>
</tr>
</tbody>
</table>
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on MX Series Routers

Starting with Junos OS Release 14.2, on MX Series routers, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

Requirements

This example uses the following hardware and software components:

- Junos OS Release 14.2 or later for MX Series routers
- One MX Series router
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the router and the RADIUS server.
• Configured 802.1X authentication on the router, with the authentication mode for interface ge-0/0/2 set to multiple.

• Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the router from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 14 on page 466, when User1 is authenticated by the MX Series router, the system creates the firewall filter `dynamic-filter-example`. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 29: Conceptual Model: Dynamic Filter Updated for Each New User

This is a conceptual model of the internal process—you cannot access or view the dynamic filter.
NOTE: If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface `ge-0/0/2` to the file server, which is located on subnet `192.0.2.16/28`, and set policer definitions to rate limit the traffic. Figure 15 on page 467 shows the network topology for this example.

Figure 30: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server

---

**Configuration**

IN THIS SECTION

- Configuring Firewall Filters on Interfaces with Multiple Supplicants | 647
To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

**Configuring Firewall Filters on Interfaces with Multiple Supplicants**

**CLI Quick Configuration**
To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols authentication-access-control interface ge-0/0/2 supplicant multiple
set firewall family bridge filter filter1 term term1 from destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall family bridge filter filter1 term term1 then count counter1
set firewall family bridge filter filter1 term term2 then policer p1
```

**Step-by-Step Procedure**
To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface `ge-0/0/2` for multiple supplicant mode authentication:

   ```
   [edit protocols]
   user@router# set authentication-access-control interface ge-0/0/2 supplicant multiple
   ```

2. Set policer definition:

   ```
   user@router# show policer p1 |display set
   set firewall policer p1 if-exceeding bandwidth-limit 1m
   set firewall policer p1 if-exceeding burst-size-limit 1k
   set firewall policer p1 then discard
   ```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

   ```
   [edit firewall family bridge]
   user@router# set filter filter1 term term1 from destination-address 192.0.2.16/28
   user@router# set filter filter1 term term1 then count counter1
   user@router# set filter filter1 term term2 then policer p1
   ```
Results

Check the results of the configuration:

```
user@router> show configuration

firewall {
    family bridge {
        filter filter1 {
            term term1 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
            }
            then count counter1;
            term term2 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
            }
            then policer p1;
        }
        policer p1 {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 1k;
            }
            then discard;
        }
    }
    protocols {
        authentication-access-control {
            interface ge-0/0/2 {
                supplicant multiple;
            }
        }
    }
}```
Verification

IN THIS SECTION
- Verifying Firewall Filters on Interfaces with Multiple Supplicants | 649

To confirm that the configuration is working properly, perform these tasks:

Verifying Firewall Filters on Interfaces with Multiple Supplicants

Purpose
Verify that firewall filters are functioning on the interface with multiple supplicants.

Action
1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on ge-0/0/2:

   user@router> show dot1x firewall

   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100

2. When a second user, User2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

   user@router> show dot1x firewall

   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/0/2_user1 100
   counter1_dot1x_ge-0/0/0/2_user2 400

Meaning
The results displayed by the show dot1x firewall command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.
<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, on MX Series routers, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server.</td>
</tr>
</tbody>
</table>
Device Discovery

Device Discovery Using LLDP and LLDP-MED on Switches | 653
NetBIOS Snooping on EX Series Switches | 669
Device Discovery Using LLDP and LLDP-MED on Switches

The Link Layer Discovery Protocol (LLDP) is an industry-standard, vendor-neutral method to allow networked devices to advertise capabilities, identity, and other information onto a LAN. It also provides additional TLVs for capabilities discovery, network policy, Power over Ethernet (PoE), and inventory management. For more information, read this topic.

Understanding LLDP

The device uses Link Layer Discovery Protocol (LLDP) to learn and distribute device information on network links. The information enables the switch to identify a variety of devices quickly. This quick identification results in a LAN that interoperate smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in Junos OS.

The device supports the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—The user-configured port description. The port description can be a maximum of 256 characters.
• **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.

• **System Description**—The system description containing information about the software and current image running on the system. This information cannot be configured, but is taken from the software.

• **System Capabilities**—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.

• **Management Address**—The IP management address of the local system.

The device supports the following 802.3 TLVs:

• **Power via MDI**—A TLV that advertises media dependent interface (MDI) power support, power source equipment (PSE) power pair, and power class information.

• **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information cannot be configured, but is based on the physical interface structure.

• **Link Aggregation**—A TLV that advertises whether the port is aggregated and its aggregated port ID.

• **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.

• **Port Vlan**—A TLV that advertises the VLAN name configured on the interface.

### Configuring LLDP (CLI Procedure)

Devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

- Enabling LLDP on Interfaces | 655
- Adjusting LLDP Advertisement Settings | 655
- Adjusting SNMP Notification Settings of LLDP Changes | 656
- Specifying a Management Address for the LLDP Management TLV | 657
- Configuring LLDP Power Negotiation | 657
- Disabling LLDP TLVs | 658
Enabling LLDP on Interfaces

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:

  ```
  [edit protocols lldp]
  user@switch# set interface all
  ```

- To configure LLDP on a specific interface:

  ```
  [edit protocols lldp]
  user@switch# set interface interface-name
  ```

Adjusting LLDP Advertisement Settings

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not change the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):

  ```
  [edit protocols lldp]
  user@switch# set advertisement-interval seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@switch# set advertisement-interval 45
  ```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the advertisement-interval value):

  ```
  [edit protocols lldp]
  user@switch# set hold-multiplier seconds
  ```

  For example, using the default value:

  ```
  [edit protocols lldp]
  user@switch# set hold-multiplier 5
  ```

- To specify the number of seconds the device waits before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled
by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds (if the advertisement-interval value is set to 8 seconds or more) or 1 second (if the advertisement-interval value is set to less than 8 seconds).

[edit protocols lldp]
user@switch# set transmit-delay seconds

For example:

[edit protocols lldp]
user@switch# set transmit-delay 2

NOTE: The advertisement-interval value must be greater than or equal to four times the transmit-delay value; otherwise, an error is returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to 0, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):

  [edit protocols lldp]
  user@switch# set lldp-configuration-notification-interval seconds

  For example:

  [edit protocols lldp]
  user@switch# set lldp-configuration-notification-interval 600

- To configure the time interval for SNMP trap notifications to wait for topology changes (in seconds):

  [edit protocols lldp]
  user@switch# set ptopo-configuration-trap-interval seconds

  For example:

  [edit protocols lldp]
  user@switch# set ptopo-configuration-trap-interval 600
• To specify the holding time (used in combination with the `ptopo-configuration-trap-interval` value) to maintain dynamic topology entries (in seconds):

```
[edit protocols lldp]
user@switch# set ptopo-configuration-maximum-hold-time seconds
```

For example:

```
[edit protocols lldp]
user@switch# set ptopo-configuration-maximum-hold-time 2147483647
```

### Specifying a Management Address for the LLDP Management TLV

You can configure an IPv4 or IPv6 management address to be used in the LLDP Management Address type, length, and value (TLV) messages. Only an out-of-band management address must be used as the value for the `management-address` statement.

To configure the management address:

```
[edit protocols lldp]
user@switch# set management-address ip-address
```

**NOTE:** Ensure that the interface with the configured management address has LLDP enabled using the `set protocols lldp interface` command. If you configure a customized management address for LLDP on an interface that has LLDP disabled, the `show lldp local-information` command output does not display the correct interface information.

### Configuring LLDP Power Negotiation

LLDP power negotiation enables the switch’s Power over Ethernet (PoE) controller to dynamically allocate PoE power to PoE interfaces, based on the needs of the powered device, by negotiating with LLDP-enabled powered devices.

**NOTE:** LLDP power negotiation is not supported on EX3200 or EX4200 switches (except for the EX4200-PX models).

LLDP power negotiation is supported on switches running PoE controller software version 4.04 or later. For information about upgrading the PoE controller software, see [Upgrading the PoE Controller Software](#).
LLDP power negotiation is automatically enabled when the PoE management mode is set to class:

- [edit poe]
  user@switch# set management class

To disable LLDP power negotiation:

- On switch interfaces:
  
  [edit protocols lldp interface all power-negotiation]
  user@switch# disable

- On a specific switch interface:
  
  [edit protocols lldp interface interface-name power-negotiation]
  user@switch# disable

Disabling LLDP TLVs

LLDP sends TLV messages by default. You can configure LLDP to disable non-mandatory TLVs. Mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- **tlv-select**—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
- **tlv-filter**—Filter the TLVs that should not be advertised by LLDP. This approach is useful if you want to filter only few TLVs, and allow everything else.

  
  **NOTE:** The **tlv-select** and **tlv-filter** are mutually exclusive and cannot be used on the same configuration stanza at the same time.

You can disable TLVs on a specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over global the global configuration.

To select which TLVs are allowed to be advertised by LLDP:

- On all interfaces:
  
  [edit protocols lldp]
  user@switch# set tlv-select tlv-name
• On a specific interface:

    [edit protocols lldp]
    user@switch#  set interface interface-name tlv-select tlv-name

To filter TLVs that should not be advertised by LLDP:

• On all interfaces:

    [edit protocols lldp]
    user@switch#  set tlv-filter tlv-name

• On a specific interface:

    [edit protocols lldp]
    user@switch#  set interface interface-name tlv-filter tlv-name

The following example disables all TLVs except port-description:

    [edit protocols lldp]
    user@switch#  set tlv-select port-description

The following example disables the system-description TLV on ge-2/1/1 interface:

    [edit protocols lldp]
    user@switch#  set interface ge-2/1/1 tlv-filter system-description

The following example disables all TLVs except port-description and system-description on all interfaces except on the ge-0/0/1 interface, where it disables only the system-name TLV:

    [edit protocols lldp]
    user@switch#  set tlv-select [port-description system-description]
    user@switch#  set interface ge-0/0/1 tlv-filter system-name

You can also disable TLVs for the LLDP Media Endpoint Discovery (LLDP-MED) protocol. See “Configuring LLDP-MED (CLI Procedure)” on page 665 for more information.
Configuring LLDP (J-Web Procedure)

NOTE: This topic applies only to the J-Web Application package.

Use the LLDP Configuration page to configure LLDP global and port settings for an EX Series switch on the J-Web interface.

To configure LLDP:

1. Select Configure > Switching > LLDP.
   
   The LLDP Configuration page displays LLDP Global Settings and Port Settings.
   
   The second half of the screen displays operational details for the selected port.

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

2. For an EX8200 Virtual Chassis configuration, select the member and the slot (FPC) from the list.

3. To modify LLDP Global Settings, click Global Settings.
   
   Enter information as described in Table 41 on page 660.

4. To modify Port Settings, click Edit in the Port Settings section.
   
   Enter information as described in Table 42 on page 661.

Table 41: Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising interval</td>
<td>Specifies the frequency of outbound LLDP advertisements. You can increase or decrease this interval.</td>
<td>Type the number of seconds.</td>
</tr>
<tr>
<td>Hold multiplier</td>
<td>Specifies the multiplier factor to be used by an LLDP-enabled switch to calculate the time-to-live (TTL) value for the LLDP advertisements it generates and transmits to LLDP neighbors.</td>
<td>Type the required number in the field.</td>
</tr>
</tbody>
</table>
Table 41: Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast start count</td>
<td>Specifies the number of LLDP advertisements sent in the first second after the device connects. The default is 3. Increasing this number results in the port initially advertising LLDP-MED at a faster rate for a limited time.</td>
<td>Type the Fast start count.</td>
</tr>
</tbody>
</table>

Table 42: Edit Port Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Status</td>
<td>Specifies whether LLDP has been enabled on the port.</td>
<td>Select one: <strong>Enabled</strong>, <strong>Disabled</strong>, or <strong>None</strong>.</td>
</tr>
<tr>
<td>LLDP-MED Status</td>
<td>Specifies whether LLDP-MED has been enabled on the port.</td>
<td>Select <strong>Enable</strong> from the list.</td>
</tr>
</tbody>
</table>

Understanding LLDP and LLDP-MED on EX Series Switches

**IN THIS SECTION**
- Benefits of LLDP and LLDP-MED    | 661
- LLDP and LLDP-MED Overview       | 662
- Supported LLDP TLVs              | 662
- Supported LLDP-MED TLVs          | 664
- Disabling TLVs                   | 665

EX Series Ethernet Switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information enables the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

**Benefits of LLDP and LLDP-MED**
- Enables the switch to quickly identify a variety of devices.
• Provides PoE power management capabilities.
• Ensures that voice traffic gets tagged and prioritized with the correct values at the source itself.

**LLDP and LLDP-MED Overview**

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone.

**NOTE:** If your IP telephone is configured for VoIP (VoIP), the switch automatically detects the configuration and assigns the telephone to the voice VLAN. The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the switch to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the switch interface to which it connects.

The switch also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

**Supported LLDP TLVs**

EX Series switches and QFX5100 switches support the following basic management TLVs:
• Chassis ID—The MAC address associated with the local system.

NOTE: The Chassis ID TLV has a subtype for the network address family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the show lldp neighbors command, but is not assigned to the VLAN.

• Port ID—The port identification for the specified port in the local system.

• Time to Live—The length of time that the received information should remain valid.

• Port Description—Textual description of the interface or the logical unit. The description for the logical unit is used, if available; otherwise, the Port Description TLV contains the description configured on the physical interface. For example, LAG member interfaces do not contain a logical unit; therefore, only the description configured on the physical interface can be used.

• System Name—The user-configured name of the local system. The system name can be a maximum of 256 characters. The system name field contains the host name and the domain name in the following format: host-name.domain-name.

• System Description—The system description that contains information about the software and current image running on the system. This information is not configurable, but taken from the software.

• System Capabilities—The primary function performed by the system. The capabilities that the system supports—for example, bridge or router. This information is not configurable, but based on the model of the product.

• Management Address—The IPv4 or IPv6 management address of the local system.

EX Series switches and QFX5100 switches support the following organizationally defined TLVs:

• Power via MDI—A TLV that advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.

• MAC/PHY Configuration Status—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type. The information is not configurable, but based on the physical interface structure.

NOTE: The MAC/PHY Configuration Status TLV has a subtype for the PMD Auto-Negotiation Advertised Capability field. This field contains a value of other or unknown if the LLDP packet is transmitted from a 10-gigabit SFP+ port.

• Link Aggregation—A TLV that advertises whether the port is aggregated and its aggregated port ID.
• Maximum Frame Size—A TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.

• Port Vlan—A TLV that advertises the VLAN name configured on the interface.

**Supported LLDP-MED TLVs**

EX Series switches and QFX5100 switches support the following LLDP-MED TLVs:

• LLDP MED Capabilities—A TLV that advertises the primary function of the port. The values of capabilities range from 0 through 15:
  • 0—Capabilities
  • 1—Network Policy
  • 2—Location Identification
  • 3—Extended Power via MDI-PSE
  • 4—Inventory
  • 5-15—Reserved

• LLDP-MED Device Class Values—Categorizes media endpoint devices into classes:
  • 0—Class not defined
  • 1—Class 1 (generic endpoints). This class definition is applicable to all endpoints that require the base LLDP discovery services.
  • 2—Class 2 (media endpoints). This class includes endpoints that have IP media capabilities.
  • 3—Class 3 (communication endpoints). Devices acting as end user communication appliances
  • 4—Network Connectivity Device
  • 5-255—Reserved

• Network Policy—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.

• Endpoint Location— A TLV that advertises the physical location of the endpoint.

• Extended Power via MDI— A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.
Disabling TLVs

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live. All other TLVs can be disabled, either on specific interfaces or on a global basis. See "Configuring LLDP (CLI Procedure)" on page 654 and "Configuring LLDP-MED (CLI Procedure)" on page 665 for more information.

SEE ALSO

Understanding PoE on EX Series Switches

Configuring LLDP-MED (CLI Procedure)

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The EX Series switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is enabled by default on EX Series switches.

This topic describes:

- Enabling LLDP-MED on Interfaces | 665
- Configuring Location Information Advertised by the Switch | 666
- Configuring a Fast Start for LLDP-MED | 666
- Disabling LLDP-MED TLVs | 667

Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

NOTE: On switches running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, configure LLDP-MED on the physical interface—for example, on ge-0/0/2. For more about ELS, see Using the Enhanced Layer 2 Software CLI.
To configure LLDP-MED on all interfaces or on a specific interface:

[edit protocols lldp-med]
user@switch# set interface interface-name

**Configuring Location Information Advertised by the Switch**

You can configure the location information that is advertised from the switch to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

  [edit protocols lldp-med]
  user@switch# set interface ge-0/0/2.0 location civic-based country-code country-code
  user@switch# set interface ge-0/0/2.0 location civic-based ca-type ca-type ca-value ca-value

- To specify a location by using an elin string:

  [edit protocols lldp-med]
  user@switch# set interface ge-0/0/2.0 location elin 4085551212

**Configuring a Fast Start for LLDP-MED**

When the switch detects an LLDP-MED capable device, it begins to send LLDP advertisements from the port connected to the device. The fast start count indicates how many advertisements will be send in the first second after the switch detects the LLDP-MED device. The default is 3; to set it to another value:

[edit protocols lldp-med]
user@switch# set fast-start seconds

For example:

[edit protocols lldp-med]
user@switch# set fast-start 6
NOTE: If an interface is configured as a VoIP interface, then the switch does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Disabling LLDP-MED TLVs

LLDP-MED sends TLV messages by default. You can configure LLDP-MED to disable non-mandatory TLVs. Mandatory TLVs are: chassis-id, port-id, and time-to-live. In this procedure, any reference to disabling all TLVs means disabling all non-mandatory TLVs.

There are two options for disabling TLVs:

- **tlv-select**—Select which TLVs are allowed to be advertised by LLDP. This approach is useful if you want to allow only a few TLVs and nothing else.
- **tlv-filter**—Filter the TLVs that should not be advertised by LLDP. This approach is useful if you want to filter only few TLVs, and allow everything else.

NOTE: The **tlv-select** and **tlv-filter** are mutually exclusive and cannot be used on the same configuration stanza at the same time.

You can disable TLVs on a specific interfaces or on all interfaces. The configuration under the interface configuration stanza takes precedence over global the global configuration.

To select which TLVs are allowed to be advertised by LLDP-MED:

- On all interfaces:

  ```
  [edit protocols lldp-med]
  user@switch# set tlv-select tlv-name
  ```

- On a specific interface:

  ```
  [edit protocols lldp-med]
  user@switch# set interface interface-name tlv-select tlv-name
  ```

To filter TLVs that should not be advertised by LLDP-MED:

- On all interfaces:
[edit protocols lldp-med]
user@switch#  set tlv-filter tlv-name

- On a specific interface:

  [edit protocols lldp-med]
  user@switch#  set interface interface-name tlv-filter tlv-name

The following example disables all TLVs except location-id:

  [edit protocols lldp-med]
  user@switch#  set tlv-select location-id

The following example disables the ext-power-via-mdi TLV on ge-2/1/1 interface:

  [edit protocols lldp-med]
  user@switch#  set interface ge-2/1/1 tlv-filter ext-power-via-mdi

The following example disables all TLVs except location-id and ext-power-via-mdi on all interfaces except on the ge-0/0/1 interface, where it disables only the network-policy TLV:

  [edit protocols lldp-med]
  user@switch#  set tlv-select [location-id ext-power-via-mdi]
  user@switch#  set interface ge-0/0/1 tlv-filter network-policy

You can also disable TLVs for the LLDP protocol. See "Configuring LLDP (CLI Procedure)" on page 654 for more information.

SEE ALSO

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch with ELS Support | 558

RELATED DOCUMENTATION

- VoIP on EX Series Switches | 525
NetBIOS Snooping on EX Series Switches

IN THIS SECTION
- Understanding NetBIOS Snooping | 669
- Configuring NetBIOS Snooping (CLI Procedure) | 670

NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch. The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database. For more information, read this topic.

Understanding NetBIOS Snooping

IN THIS SECTION
- What Is a NetBIOS Name? | 669
- How NetBIOS Snooping Works | 670

NetBIOS snooping allows Juniper Networks EX Series Ethernet Switches to discover NetBIOS hosts that are connected to the switch.

What Is a NetBIOS Name?

A NetBIOS name is a key element in communications between NetBIOS resources. A NetBIOS name identifies a NetBIOS resource on the network. A NetBIOS name is either a unique (exclusive) name or a group (nonexclusive) name. When a NetBIOS resource communicates with one other NetBIOS resource, a unique name is used in that communication. When a NetBIOS resource communicates with multiple resources, a group name is used.

The NetBIOS name of each NetBIOS resource is stored on the NetBIOS Name Server (NBNS). The NetBIOS name of a NetBIOS resource is mapped to its IP address.
A NetBIOS name is a 16-byte address. The first 15 bytes contain the name and the last byte contains the name type.

The NetBIOS name service is supported over UDP port 137.

How NetBIOS Snooping Works

You can enable NetBIOS snooping on the switch so that the switch can identify NetBIOS resources that are connected to it.

When a host connected to the switch initializes itself, it attempts to register its NetBIOS name by sending a NetBIOS name registration request message. The host can opt for either a unique or a group NetBIOS name. For a unique NetBIOS name, the host either broadcasts a NetBIOS name query message on the local network or unicasts it to the NBNS to check whether the requested name is already being used by another host. If so, the host that previously registered the name or the NBNS responds with a negative name registration response. If the host receives no negative response, it broadcasts the NetBIOS name registration packet to confirm the name. For a NetBIOS group name, the host sends a NetBIOS name registration packet, which generates no responses from other hosts because multiple hosts can use the same group name at the same time.

The NetBIOS snooping-enabled switch extracts the host details from the NetBIOS name registration packet and stores the details in the LLDP neighbor database.

SEE ALSO

Understanding LLDP and LLDP-MED on EX Series Switches | 661

Configuring NetBIOS Snooping (CLI Procedure)

IN THIS SECTION

- Enabling NetBIOS Snooping | 671
- Disabling NetBIOS Snooping | 671
NetBIOS snooping enables an EX Series switch to learn information about NetBIOS hosts that are connected to the switch.

This topic describes:

**Enabling NetBIOS Snooping**

To enable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# set netbios-snooping
```

**Disabling NetBIOS Snooping**

To disable NetBIOS snooping:

```
[edit protocols lldp]
user@switch# delete netbios-snooping
```

SEE ALSO

- `show lldp neighbors` | 2697

RELATED DOCUMENTATION

- `netbios-snooping` | 1985
Domain Name Security

DNSSEC Overview | 675
Configuring the TTL Value for DNS Server Caching | 675
Example: Configuring DNSSEC | 677
Example: Configuring Secure Domains and Trusted Keys for DNSSEC | 678
Example: Configuring Keys for DNSSEC | 680
DNS Proxy Overview | 681
Configuring the Device as a DNS Proxy | 686
DNSSEC Overview

Junos OS devices support the domain name service security extensions (DNSSEC) standard. DNSSEC is an extension of DNS that provides authentication and integrity verification of data by using public-key based signatures.

In DNSSEC, all the resource records in a DNS are signed with the private key of the zone owner. The DNS resolver uses the public key of the owner to validate the signature. The zone owner generates a private key to encrypt the hash of a set of resource records. The private key is stored in RRSIG record. The corresponding public key is stored in the DNSKEY record. The resolver uses the public key to decrypt the RRSIG and compares the result with the hash of the resource record to verify that it has not been altered.

Similarly, the hash of the public DNSKEY is stored in a DS record in a parent zone. The zone owner generates a private key to encrypt the hash of the public key. The private key is stored in the RRSIG record. The resolver retrieves the DS record and its corresponding RRSIG record and public key. Using the public key, the resolver decrypts the RRSIG record and compares the result with the hash of the public DNSKEY to verify that it has not been altered. This establishes a chain of trust between the resolver and the name servers.

RELATED DOCUMENTATION

| DNS Overview |
| Example: Configuring Keys for DNSSEC | 680 |
| Example: Configuring Secure Domains and Trusted Keys for DNSSEC | 678 |

Configuring the TTL Value for DNS Server Caching

IN THIS SECTION
- Requirements | 676
- Overview | 676
- Configuration | 676
- Verification | 677
This section describes how to configure the TTL value for a DNS server cache to define the period for which DNS query results are cached.

**Requirements**

No special configuration beyond device initialization is required before performing this task.

**Overview**

The DNS name server stores DNS query responses in its cache for the TTL period specified in the TTL field of the resource record. When the TTL value expires, the name server sends a fresh DNS query and updates the cache. You can configure the TTL value from 0 to 604,800 seconds. You can also configure the TTL value for cached negative responses. Negative caching is the storing of the record that a value does not exist. In this example, you set the maximum TTL value for cached (and negative cached) responses to 86,400 seconds.

**Configuration**

**Step-by-Step Procedure**

To configure the TTL value for a DNS server cache:

1. Specify the maximum TTL value for cached responses, in seconds. (In this example, 86400 seconds equals 24 hours.)

   ```
   [edit]
   user@host# set system services dns max-cache-ttl 86400
   ```

2. Specify the maximum TTL value for negative cached responses, in seconds.

   ```
   [edit]
   user@host# set system services dns max-ncache-ttl 86400
   ```

3. If you are done configuring the device, commit the configuration.

   ```
   [edit]
   ```
Verification

To verify the configuration is working properly, enter the `show system services` command.

RELATED DOCUMENTATION

| DNS Overview |

Example: Configuring DNSSEC

DNS-enabled devices run a DNS resolver (proxy) that listens on loopback address 127.0.0.1 or ::1. The DNS resolver performs a hostname resolution for DNSSEC. Users need to set name server IP address to 127.0.0.1 or ::1 so the DNS resolver forwards all DNS queries to DNSSEC instead of to DNS. If the name server IP address is not set, DNS will handle all queries instead of to DNSSEC.

The following example shows how to set the server IP address to 127.0.0.1:

```
[edit]
user@host# set system name-server 127.0.0.1
```

The DNSSEC feature is enabled by default. You can disable DNSSEC in the server by using the following CLI command:

```
[edit]
set system services dns dnssec disable
```

RELATED DOCUMENTATION

| DNSSEC Overview | 675 |
Example: Configuring Secure Domains and Trusted Keys for DNSSEC

IN THIS SECTION

- Requirements | 678
- Overview | 678
- Configuration | 679

This example shows how to configure secure domains and trusted keys for DNSSEC.

Requirements

Set the name server IP address so the DNS resolver forwards all DNS queries to DNSSEC instead of DNS. See “Example: Configuring DNSSEC” on page 677 for more information.

Overview

You can configure secure domains and assign trusted keys to the domains. Both signed and unsigned responses can be validated when DNSSEC is enabled.

When you configure a domain as a secure domain and if DNSSEC is enabled, all unsigned responses to that domain are ignored and the server returns a SERVFAIL error code to the client for the unsigned responses. If the domain is not configured as a secure domain, unsigned responses will be accepted.

When the server receives a signed response, it checks if the DNSKEY in the response matches any of the trusted keys that are configured. If it finds a match, the server accepts the signed response.

You can also attach a DNS root zone as a trusted anchor to a secure domain to validate the signed responses. When the server receives a signed response, it queries the DNS root zone for a DS record. When it receives the DS record, it checks if the DNSKEY in the DS record matches the DNSKEY in the signed response. If it finds a match, the server accepts the signed response.
Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system services dns dnssec secure-domains domain1.net
set system services dns dnssec secure-domains domain2.net
set system services dns dnssec trusted-keys key domain1.net.ABC123ABCh
set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
```

Step-by-Step Procedure
To configure secured domains and trusted keys for DNSSEC:

1. Configure domain1.net and domain2.net as secure domains.

   ```
   [edit]
   user@host# set system services dns dnssec secure-domains domain1.net
   user@host# set system services dns dnssec secure-domains domain2.net
   ```

2. Configure trusted keys to domain1.net.

   ```
   [edit]
   user@host# set system services dns dnssec trusted-keys key "domain1.net.ABC123ABCh"
   ```

3. Attach a root zone dlv.isc.org as a trusted anchor to a secure domain.

   ```
   [edit]
   user@host# set system services dns dnssec dlv domain domain2.net trusted-anchor dlv.isc.org
   ```

Results
From configuration mode, confirm your configuration by entering the show system services command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dns {
    dnssec {
        trusted-keys {
```
If you are done configuring the device, enter **commit** from configuration mode.

**Example: Configuring Keys for DNSSEC**

You can load a public key from a file or you can copy and paste the key file from a terminal. In both cases, you must save the keys to the configuration instead of to a file. The following example shows how to load a key from a file:

```
[edit system services dns dnssec trusted-keys]
#load-key filename
```

The following example explains how to load the key from a terminal:

```
[edit system services dns dnssec trusted-keys]
# set key "...pasted-text...
```

If you are done loading the keys from the file or terminal, click **commit** in the CLI editor.
DNS Proxy Overview

A dynamic name system (DNS) proxy allows clients to use an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved.

DNS Proxy Cache

When a DNS query is resolved by a DNS proxy, the result is stored in the device's DNS cache. This stored cache helps the device to resolve subsequent queries from the same domain and avoid network latency delay.

NOTE: If the proxy cache is not available, the device sends the query to the configured DNS server, which results in network latency delays.

DNS proxy maintains a cache entry for each resolved DNS query. These entries have a time-to-live (TTL) timer so the device purges each entry from the cache as it reaches its TTL and expires. You can clear a cache by using the clear cache command, or the cache will automatically expire along with TTL when it goes to zero.
DNS Proxy with Split DNS

The split DNS proxy feature allows you to configure your proxy server to split the DNS query based on both the interface and the domain name. You can also configure a set of name servers and associate them with a given domain name. When you query that domain name, the device sends the DNS queries to only those name servers that are configured for that domain name to ensure localization of DNS queries.

You can configure the transport method used to resolve a given domain name—for example, when the device connects to the corporate network through an IPsec VPN or any other secure tunnel. When you configure a secure VPN tunnel to transport the domain names belonging to the corporate network, the DNS resolution queries are not leaked to the ISP DNS server and are contained within the corporate network.

You can also configure a set of default domain (*) and name servers under the default domain to resolve the DNS queries for a domain for which a name server is not configured.

Each DNS proxy must be associated with an interface. If an interface has no DNS proxy configuration, all the DNS queries received on that interface are dropped.

Figure 31 on page 683 shows how the split DNS proxy works in a corporate network.
In the corporate network shown in Figure 31 on page 683, a PC client that points to the SRX Series device as its DNS server makes two queries—to www.your-isp.com and to www.intranet.com. The DNS proxy redirects the www.intranet.com query to the www.intranet.com DNS server (203.0.113.253), while the www.your-isp.com query is redirected to the ISP DNS server (209.100.3.130). Although the query for
www.your-isp.com is sent to the ISP DNS server as a regular DNS query using clear text protocols (TCP/UDP), the query for the www.intranet.com domain goes to the intranet’s DNS servers over a secure VPN tunnel.

A split DNS proxy has the following advantages:

- Domain lookups are usually more efficient. For example, DNS queries meant for a corporate domain (such as acme.com) can go to the corporate DNS server exclusively, while all others go to the ISP DNS server. Splitting DNS lookups reduces the load on the corporate server and can also prevent corporate domain information from leaking onto the Internet.

- A DNS proxy allows you to transmit selected DNS queries through a tunnel interface, which prevents malicious users from learning about the internal configuration of a network. For example, DNS queries bound for the corporate server can pass through a tunnel interface to use security features such as authentication and encryption.

---

Dynamic Domain Name System Client

Dynamic DNS (DDNS) allows clients to dynamically update IP addresses for registered domain names. This feature is useful when an ISP uses Point-to-Point Protocol (PPP), Dynamic Host Configuration Protocol (DHCP), or external authentication (XAuth) to dynamically change the IP address for a customer premises equipment (CPE) router (such as a security device) that protects a Web server. Internet clients can reach the Web server by using a domain name even if the IP address of the security device has previously changed dynamically.

A DDNS server maintains a list of the dynamically changed addresses and their associated domain names. The device updates these DDNS servers with this information periodically or in response to IP address changes. The Junos OS DDNS client supports popular DDNS servers such as dyndns.org and ddo.jp

Figure 32 on page 685 illustrates how the DDNS client works.
The IP address of the internal Web server is translated by Network Address Translation (NAT) to the IP address of the untrust zone interface on the device. The hostname abc-host.com is registered with the DDNS server and is associated with the IP address of the device's untrust zone interface, which is monitored...
by the DDNS client on the device. When the IP address of abc-host.com is changed, the DDNS server is informed of the new address.

If a client in the network shown in Figure 32 on page 685 needs to access abc-host.com, the client queries the DNS servers on the Internet. When the query reaches the DDNS server, it resolves the request and provides the client with the latest IP address of abc-host.com.

### RELATED DOCUMENTATION

| Configuring the Device as a DNS Proxy | 686 |

### Configuring the Device as a DNS Proxy

The Junos operating system (Junos OS) incorporates domain name system (DNS) support, which allows you to use domain names as well as IP addresses for identifying locations. A DNS server keeps a table of the IP addresses associated with domain names. Using DNS enables an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device to reference locations by domain name (such as www.example.net) in addition to using the routable IP address.

DNS features include:

- **DNS proxy cache**—The device proxies hostname resolution requests on behalf of the clients behind the SRX Series device. DNS proxy improves domain lookup performance by using caching.

- **Split DNS**—The device redirects DNS queries over a secure connection to a specified DNS server in the private network. Split DNS prevents malicious users from learning the network configuration, and thus also prevents domain information leaks. Once configured, split DNS operates transparently.

- **Dynamic DNS (DDNS) client**—Servers protected by the device remain accessible despite dynamic IP address changes. For example, a protected Web server continues to be accessible with the same hostname, even after the dynamic IP address is changed because of address reassignment by the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) by Internet service provider (ISP).
To configure the device as a DNS proxy, you enable DNS on a logical interface and configure DNS proxy servers. Configuring a static cache enables branch office and corporate devices to use hostnames to communicate. Configuring dynamic DNS (DDNS) clients allows IP address changes.

Perform the following procedure to configure the device as a DNS proxy server by enabling DNS proxy on a logical interface—for example, ge-2/0/0.0—and configuring a set of name servers that are to be used for resolving the specified domain names. You can specify a default domain name by using an asterisk (*) and then configure a set of name servers for resolution. Use this approach when you need global name servers to resolve domain name entries that do not have a specific name server configured.

1. DNS proxy with non-split dns configuration
   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-0/0/3.0
     ```

   - Set dns resolver to forward received dns query.

     ```
     [edit]
     user@host# set system services dns forwarders 192.0.2.0
     ```

   - If you are done configuring the device, commit the configuration.

     ```
     [edit]
     user@host# commit
     ```

     To verify if the configuration is working properly, execute the show command.

     ```
     user@host# show system services dns dns-proxy
     ```

2. DNS proxy with split dns configuration
   - Enable DNS proxy on a logical interface.

     ```
     [edit]
     user@host# set system services dns dns-proxy interface ge-2/0/0.0
     ```

   - Configure view for split DNS, specify the internal IP interface to handle the DNS query and view the logical subnet address.

     ```
     [edit]
     user@host# set system services dns dns-proxy view internal match-clients 1.1.1.0/24
     ```
• Set a default internal domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

[edit]
user@host# set system services dns dns-proxy view internal domain aa.internal.com forwarders 1.1.1.1
user@host# set system services dns dns-proxy view internal domain bb.internal.com forwarders 2.2.2.2

• Configure view for split DNS, specify the external IP interface to handle the DNS query and view the logical subnet address.

[edit]
user@host# set system services dns dns-proxy view external match-clients 11.1.1.0/24

• Set a default external domain name, and specify IP server for forwarding the DNS query according to their IP addresses.

[edit]
user@host# set system services dns dns-proxy view external domain aa.external.com forwarders 3.3.3.3
user@host# set system services dns dns-proxy view external domain bb.external.com forwarders 4.4.4.4

• If you are done configuring the device, commit the configuration.

[edit]
user@host# commit

To verify if the configuration is working properly, execute the show command.

user@host# show system services dns dns-proxy

3. DNS proxy cache configuration

• Configure the dns proxy static cache entries to specify the host’s IPv4 address.

[edit]
user@host# set system services dns dns-proxy cache aa.example.net inet 10.10.10.10
user@host# set system services dns dns-proxy cache bb.example.net inet 20.20.20.20

• If you are done configuring the device, commit the configuration.

[edit]
user@host# commit
To verify if the configuration is working properly, execute the show command.

```
user@host# show system services dns dns-proxy
```

4. Dynamic DNS proxy configuration

- Enable client.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface ge-2/0/0.0 username test password test123
```

- Configure the server.

```
[edit]
user@host# set system services dynamic-dns client abc.com agent juniper interface ge-2/0/0.0 username test password test123 server ddo
user@host# set system services dynamic-dns client abc.com agent juniper interface ge-2/0/0.0 username test password test123 server dyndns
```

- If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

To verify if the configuration is working properly

```
user@host# show system services dynamic-dns client
```

RELATED DOCUMENTATION

- Configuring the Device as a DNS Proxy | 686
CHAPTER 11

DHCP on Routers

DHCP for Routing Devices | 693
DHCP Local Server | 700
Extended DHCP Local Server | 717
Using DHCP Relay Agent Option 82 Information | 739
A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A Junos OS device acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. For more information, read this topic.
DHCP access service consists of two components: a protocol for delivering host-specific configuration information from a server to a client host and a method for allocating network addresses to a client host. The client sends a message to request configuration information. A DHCP server sends the configuration information back to the client.

With DHCP, clients can be assigned a network address for a fixed lease, enabling serial reassignment of network addresses to different clients. A DHCP server leases IP addresses for specific times to various clients. If a client does not use its assigned address for some period of time, the DHCP server can assign that IP address to another host. When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The DHCP server includes IPv4 address assignment and commonly used DHCP options. The server is compatible with DHCP servers from other vendors on the network. The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The Junos-FIPS software does not support the DHCP server.

NOTE: You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.

The following topics describe these concepts in detail:

**Network Address Assignments (Allocating a New Address)**

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.
1. When a client computer is started, it broadcasts a **DHCPDISCOVER** message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

![DHCP Discover Diagram](Image)

**NOTE:** For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes **DHCPDISCOVER** messages even if the overload options in the messages are not properly terminated with an `end` statement.

2. Each DHCP server receiving the broadcast sends a **DHCPOFFER** message to the client, offering an IP address for a set period of time, known as the lease period.

![DHCP Offer Diagram](Image)

3. The client receives one or more **DHCPOFFER** messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.

4. The client broadcasts a **DHCPREQUEST** message indicating the client has selected an offered leased IP address and identifies the selected server.

![DHCP Request Diagram](Image)

5. Those servers not selected by the **DHCPREQUEST** message return the unselected IP addresses to the pool of available addresses.
6. The selected DHCP server sends a **DHCPACK** acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

Figure 36: DHCP ACK

7. The client receives the **DHCPACK** message with configuration information. The process is complete. The client is configured and has access to the network.
   - If the client receives a **DHCPNAK** message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.
   - The client can relinquish its lease on a network address by sending a **DHCPRELEASE** message to the server (for example, when the client is restarted). When the server receives the **DHCPRELEASE** message, it marks the lease as free and the IP address becomes available again.

Figure 37: DHCP Release

**Network Address Assignments (Reusing a Previously Assigned Address)**

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a **DHCPREQUEST** message on the local subnet.
2. The server with knowledge of the client's configuration responds with a **DHCPACK** message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.
Static and Dynamic Bindings

DHCP supports both dynamic and static bindings. For dynamic bindings, IP addresses are assigned to clients from a pool of addresses. Static bindings provide configuration information for a specific client and can include one or more fixed IP addresses for the client. You can configure a DHCP server to include both address pools and static bindings. For any individual client, static bindings take priority over address pools.

Compatibility with Autoinstallation

The DHCP server is compatible with the autoinstallation feature on J Series Services Routers. The server automatically checks autoinstallation settings for conflicts and gives autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes priority over an IP address set by the DHCP server.

NOTE: The autoinstallation feature includes a fixed address pool and a fixed lease time. With DHCP, you can create address pools and modify lease times.

Conflict Detection and Resolution

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the `clear system services dhcp conflict` command.

DHCP Statement Hierarchy and Inheritance

DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients. See Table 43 on page 698.

The `pool` and `static-binding` statements appear at the `edit system services dhcp` hierarchy level. You can include the remaining statements at the following hierarchy levels:
Table 43: Pool and Binding Statements

<table>
<thead>
<tr>
<th>Statement</th>
<th>Description</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool</td>
<td>Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.</td>
<td>[edit system services dhcp]</td>
</tr>
<tr>
<td>static-binding</td>
<td>Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client’s MAC address.</td>
<td></td>
</tr>
</tbody>
</table>

To minimize configuration changes, include common configuration statements shown in Table 44 on page 699 (for example, the domain-name statement) at the highest applicable level of the hierarchy (network or subnetnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the [edit system services dhcp] and [edit system services dhcp pool] hierarchy levels, the value assigned to the statement at the [edit system services dhcp pool] level takes priority.
<table>
<thead>
<tr>
<th>Statement</th>
<th>Description</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot-file</code></td>
<td>Set the boot filename advertised to clients. The client uses the boot image stored in the boot file to complete configuration.</td>
<td>[edit system services dhcp] [edit system services dhcp pool] [edit system services dhcp static-binding]</td>
</tr>
<tr>
<td><code>boot-server</code></td>
<td>Set the server that contains the boot file.</td>
<td></td>
</tr>
<tr>
<td><code>default-lease-time</code></td>
<td>Set the default lease time assigned to any client that does not request a specific lease time.</td>
<td></td>
</tr>
<tr>
<td><code>domain-name</code></td>
<td>Configure the name of the domain in which clients will search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.</td>
<td></td>
</tr>
<tr>
<td><code>domain-search</code></td>
<td>Define a domain search list.</td>
<td></td>
</tr>
<tr>
<td><code>maximum-lease-time</code></td>
<td>Set the maximum lease time allowed by the server.</td>
<td></td>
</tr>
<tr>
<td><code>name-server</code></td>
<td>Specify the DNS server that maintains the database of client name to IP address mappings.</td>
<td></td>
</tr>
<tr>
<td><code>option</code></td>
<td>Configure user-defined DHCP options.</td>
<td></td>
</tr>
<tr>
<td><code>router</code></td>
<td>Specify IP address for routers on the client’s subnetwork. Routers are listed in order of preference.</td>
<td></td>
</tr>
<tr>
<td><code>server-identifier</code></td>
<td>Set the IP address of the DHCP server.</td>
<td></td>
</tr>
</tbody>
</table>
DHCP Local Server

IN THIS SECTION

- Configuring Address Pools for DHCP Dynamic Bindings | 700
- Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address | 702
- Specifying DHCP Lease Times for IP Address Assignments | 703
- Configuring a DHCP Boot File and DHCP Boot Server | 704
- Configuring a Static IP Address as DHCP Server Identifier | 705
- Configuring a Domain Name and Domain Search List for a DHCP Server Host | 706
- Configuring Routers Available to the DHCP Client | 706
- Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server | 707
- Example: Complete DHCP Server Configuration | 708
- Verifying and Managing the DHCP Server Configuration | 710
- Example: Viewing DHCP Bindings | 711
- Example: Viewing DHCP Address Pools | 712
- Example: Viewing and Clearing DHCP Conflicts | 712
- Configuring Tracing Operations for DHCP Processes | 713
- DHCP Processes Tracing Flags | 716

DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

Configuring Address Pools for DHCP Dynamic Bindings

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet.
To configure an address pool, include the following statements at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
pool address/<prefix-length> {
    address-range {
        low address;
        high address;
    }
    exclude-address {
        address;
    }
}
```

The pool definition must include the client subnet number and prefix length (in bits). Optionally, the definition can include an address range and a list of excluded addresses.

The `address-range` statement defines the lowest and highest IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

The `exclude-address` statement specifies addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit system services dhcp]
pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
    exclude-address {
        10.3.3.33;
    }
}
```

For dynamic address assignment, configure an address pool for each client subnet the DHCP server supports. You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.

DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the DHCPDISCOVER packet is received. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.
Configuring Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

To configure static bindings, include the following statements at the [edit system services dhcp] hierarchy level:

```
[edit system services dhcp]
static-binding mac-address {
    fixed-address {
        address;
    }
    host client-hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
}
```

A static binding defines a mapping between a fixed IP address and the client’s MAC address.

The `mac-address` variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The `fixed-address` statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The `host` statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the `domain-name` statement.

The `client-identifier` statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, Assigned Numbers. Either a client identifier or the client’s MAC address must be configured to uniquely identify the client on the network.

**NOTE:** For each unique `client-identifier client-id` value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect `client-identifier client-id` value, the DHCP server did not issue a lease.
The following is an example of a static binding configuration:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
  fixed-address {
    10.5.5.5;
    10.6.6.6;
  }
  host-name "another-host.domain.tld";
  client-identifier hexadecimal 01001122aabbcc;
}
```

### Specifying DHCP Lease Times for IP Address Assignments

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure lease times, include the `maximum-lease-time` and `default-lease-time` statements:

```
maximum-lease-time;
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the `[edit system services dhcp]` hierarchy level.

The `maximum-lease-time` statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.

**NOTE:** Maximum lease times do not apply to dynamicBOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.
The following example shows a configuration for maximum and default lease times:

```plaintext
[edit system services dhcp]
  maximum-lease-time 7200;
  default-lease-time 3600;
```

---

### Configuring a DHCP Boot File and DHCP Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the `boot-file` and `boot-server` statements:

```plaintext
boot-file filename;
boot-server (address | hostname);
```

You can include these statements at the following hierarchy levels:

```plaintext
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

After a client receives a **DHCP OFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

The `boot-file` statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The `boot-server` statement configures the IP address of the TFTP server that contains the client’s initial boot file. You must configure an IP address or a hostname for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the `[edit system services dhcp]` hierarchy level.

The following example specifies a boot file and server for an address pool:

```plaintext
[edit system services dhcp]
pool 10.4.4.0/24 {
```
Configuring a Static IP Address as DHCP Server Identifier

The host running the DHCP server must itself use a manually assigned, static IP address. It cannot send a request and receive an IP address from itself or another DHCP server.

To configure a DHCP server identifier, include the server-identifier statement:

```
server-identifier address;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The server-identifier statement specifies the IP address of the DHCP server. The host must be a TFTP server that is accessible by all clients served within a range of IP addresses (based on either an address pool or static binding).

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
    exclude-address {
        10.3.3.33;
    }
    router {
        10.3.3.1;
    }
    server-identifier 10.3.3.1;
}
```
Configuring a Domain Name and Domain Search List for a DHCP Server Host

To configure the name of the domain in which clients search for a DHCP server host, include the `domain-name` statement:

```
    domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The `domain-name` statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

To configure a domain search list, include the `domain-search` statement:

```
    domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The `domain-search` statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The `domain-search` statement is optional, if you do not configure a domain search list, the default is the client's current domain.

Configuring Routers Available to the DHCP Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the `router` statement:
You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The `router` statement specifies a list of IP addresses for routers on the client’s subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the `[edit system services dhcp]` hierarchy level:

```
[edit system services dhcp]
router {
    10.6.6.1;
    10.7.7.1;
}
```

---

### Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the `option` statement:

```
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

The `option` statement specifies the following values:
- **id-number**—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.

- **option-type**—Any of the following types: byte, byte-stream, flag, integer, ip-address, short, string, unsigned-integer, unsigned-short.

- **array**—An option can include an array of values.

- **option-value**—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The following example shows user-defined DHCP options:

```
[edit system services dhcp]
option 19 flag off; # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined option3 router statement and uses the router statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2; # 3: "Default Router" option
router {
    10.7.7.1;
}
```

### Example: Complete DHCP Server Configuration

This topic shows a complete DHCP server configuration with address pools, static bindings, and user-defined options.

The following example shows statements at the [edit interfaces] hierarchy level. The interface's primary address (10.3.3.1/24) has a corresponding address pool (10.3.3.0/24) defined at the [edit system services] hierarchy level.
NOTE: You can configure a DHCP server only on an interface's primary IP address. The primary address on an interface is the address that is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.

Statements at the `[edit system services]` hierarchy level include the following:

```plaintext
[edit system services]
dhcp {
    domain-name "domain.tld";
    maximum-lease-time 7200;
    default-lease-time 3600;
    name-server {
        10.6.6.6;
        10.6.6.7;
    }
    domain-search [ subnet1.domain.tld subnet2.domain.tld ];
    wins-server {
        10.7.7.7;
        10.7.7.9;
    }
    router {
        10.6.6.1;
        10.7.7.1;
    }
    option 19 flag off; # 19: "IP Forwarding" option
    option 40 string "domain.tld"; # 40: "NIS Domain" option
    option 16 ip-address 10.3.3.3; # 16: "Swap Server" option
    pool 10.3.3.0/24 {
        address-range low 10.3.3.2 high 10.3.3.254;
        exclude-address {
            10.3.3.33;
        }
    }
}
Verifying and Managing the DHCP Server Configuration

To display the client address bindings for the extended DHCP local server, use the following operational commands:

- `show dhcp server binding`
- `show dhcp server statistics`

To clear client address bindings and DHCP local server statistics, use the following operational commands:

- `clear dhcp server binding`
- `clear dhcp server statistics`

For information about using these operations commands, see the *Junos System Basics and Services Reference.*
Example: Viewing DHCP Bindings

Use the CLI command `show system services dhcp binding` to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hardware Address</th>
<th>Type</th>
<th>Lease expires at</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>00:a0:12:00:12:ab</td>
<td>static</td>
<td>never</td>
</tr>
<tr>
<td>192.168.1.3</td>
<td>00:a0:12:00:13:02</td>
<td>dynamic</td>
<td>2004-05-03 13:01:42 PDT</td>
</tr>
</tbody>
</table>
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
IP address         192.168.1.3
Hardware address   00:a0:12:00:12:ab
Client identifier  61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00 3a 31 33 3a 30 32
Lease information:
  Type     dynamic
  Obtained at 2004-05-02 13:01:42 PDT
  Expires at 2004-05-03 13:01:42 PDT
```

Use the `detail` option to show detailed binding information:

```
user@host> show system services dhcp binding detail

DHCP binding information:
IP address         192.168.1.3
Hardware address   00:a0:12:00:12:ab
Pool               192.168.1.0/24
Interface          fe-0/0/0, relayed by 192.168.4.254
Lease information:
```
Dynamic

Obtained at 2004-05-02 13:01:42 PDT
Expires at 2004-05-03 13:01:42 PDT

DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off

Example: Viewing DHCP Address Pools

Use the CLI command `show system services dhcp pool` to view information about DHCP address pools.

The following example shows address pools configured on a DHCP server:

```
user@host> show system services dhcp pool
```

<table>
<thead>
<tr>
<th>Pool name</th>
<th>Low address</th>
<th>High address</th>
<th>Excluded addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.40.1.0/24</td>
<td>10.40.1.1</td>
<td>10.40.1.254</td>
<td>10.40.1.254</td>
</tr>
</tbody>
</table>

Example: Viewing and Clearing DHCP Conflicts

When the DHCP server provides an IP address, the client performs an ARP check to make sure the address is not being used by another client and reports any conflicts back to the server. The server keeps track of addresses with conflicts and removes them from the address pool. Use the CLI command `show system services dhcp conflict` to show conflicts.

```
user@host> show system services dhcp conflict
```

<table>
<thead>
<tr>
<th>Detection time</th>
<th>Detection method</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-08-03 19:04:00 PDT</td>
<td>client</td>
<td>192.168.1.5</td>
</tr>
<tr>
<td>2004-08-04 04:23:12 PDT</td>
<td>ping</td>
<td>192.168.1.8</td>
</tr>
</tbody>
</table>

Use the command `clear system services dhcp conflict` to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```
For more information about CLI commands you can use with the DHCP server, see the CLI Explorer.

## Configuring Tracing Operations for DHCP Processes

DHCP tracing operations track all DHCP operations and record them to a log file. By default, no DHCP processes are traced. If you include the `traceoptions` statement at the `[edit system services dhcp]` hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called `dhcpd` located in the `/var/log` directory.

- When the file `dhcpd` reaches 128 kilobytes (KB), it is renamed `dhcpd.0`, then `dhcpd.1`, and so on, until there are three trace files. Then the oldest trace file (`dhcpd.2`) is overwritten. For more information about how log files are created, see the System Log Explorer.

- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the `[edit system services dhcp traceoptions]` hierarchy level:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable|no-world-readable>;
flag {
  all;
}
```

### Tasks for Configuring DHCP Tracing Operations

1. Configuring the DHCP Processes Log Filename | 713
2. Configuring the Number and Size of DHCP Processes Log Files | 714
3. Configuring Access to the DHCP Log File | 714
4. Configuring a Regular Expression for Refining the Output of DHCP Logged Events | 715
5. Configuring DHCP Trace Operation Events | 715

### Configuring the DHCP Processes Log Filename

By default, the name of the file that records trace output is `dhcpd`. You can specify a different name by including the file statement at the `[edit system services dhcp traceoptions]` hierarchy level:
Configuring the Number and Size of DHCP Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are three trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the `[edit system services dhcp traceoptions]` hierarchy level:

```plaintext
[edit system services dhcp traceoptions]
file filename;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (`filename`) reaches 2 MB, `filename` is renamed `filename.0`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0` is renamed `filename.1` and `filename` is renamed `filename.0`. This process repeats until there are 20 trace files. Then the oldest file (`filename.19`) is overwritten by the newest file (`filename.0`).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the `file world-readable` statement at the `[edit system services dhcp traceoptions]` hierarchy level:

```plaintext
[edit system services dhcp traceoptions]
file world-readable;
```

To set the default behavior explicitly, include the `file no-world-readable` statement at the `[edit system services dhcp traceoptions]` hierarchy level:

```plaintext
[edit system services dhcp traceoptions]
file no-world-readable;
```
Configuring a Regular Expression for Refining the Output of DHCP Logged Events

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit system services dhcp traceoptions file filename] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

Configuring DHCP Trace Operation Events

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
    all;
    binding;
    config;
    conflict;
    event;
    ifdb;
    io;
    lease;
    main;
    misc;
    packet;
    options;
    pool;
    protocol;
    rtsock;
    scope;
    signal;
    trace;
    ui;
}
```
### DHCP Processes Tracing Flags

Table 45 on page 716 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

Table 45: DHCP Processes Tracing Flags

<table>
<thead>
<tr>
<th>Flag</th>
<th>Operation or Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>All operations.</td>
</tr>
<tr>
<td>binding</td>
<td>Binding operations.</td>
</tr>
<tr>
<td>config</td>
<td>Logins to the configuration database.</td>
</tr>
<tr>
<td>conflict</td>
<td>Client-detected conflicts for IP addresses.</td>
</tr>
<tr>
<td>event</td>
<td>Important events.</td>
</tr>
<tr>
<td>ifdb</td>
<td>Interface database operations.</td>
</tr>
<tr>
<td>io</td>
<td>I/O operations.</td>
</tr>
<tr>
<td>lease</td>
<td>Lease operations.</td>
</tr>
<tr>
<td>main</td>
<td>Main loop operations.</td>
</tr>
<tr>
<td>misc</td>
<td>Miscellaneous operations.</td>
</tr>
<tr>
<td>packet</td>
<td>DHCP packets.</td>
</tr>
<tr>
<td>options</td>
<td>DHCP options.</td>
</tr>
<tr>
<td>pool</td>
<td>Address pool operations.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol operations.</td>
</tr>
<tr>
<td>rtsock</td>
<td>Routing socket operations.</td>
</tr>
<tr>
<td>scope</td>
<td>Scope operations.</td>
</tr>
<tr>
<td>signal</td>
<td>DHCP signal operations.</td>
</tr>
<tr>
<td>trace</td>
<td>Tracing operations.</td>
</tr>
</tbody>
</table>
Table 45: DHCP Processes Tracing Flags (continued)

<table>
<thead>
<tr>
<th>Flag</th>
<th>Operation or Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ui</td>
<td>User interface operations.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- DHCP for Switches | 751
- DHCP Overview | 909

Extended DHCP Local Server

IN THIS SECTION

- Extended DHCP Local Server Overview | 718
- Configuring the Router as an Extended DHCP Local Server | 723
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 725
- Extended DHCP Local Server and Address-Assignment Pools | 725
- Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use | 726
- Default Options Provided by the Extended DHCP Server for the DHCP Client | 727
- Using External AAA Authentication Services to Authenticate DHCP Clients | 728
- Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | 733
- Example: Configuring the Minimum Extended DHCP Local Server Configuration | 734
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching | 735
- Tracing Extended DHCP Local Server Operations | 735

An extended DHCP local server enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality. For more information, read this topic.
Extended DHCP Local Server Overview

IN THIS SECTION

- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 720
- Providing DHCP Client Configuration Information | 720
- Minimal Configuration for Clients | 722
- DHCP Local Server and Address-Assignment Pools | 722
Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. Table 46 on page 719 provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 46: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

<table>
<thead>
<tr>
<th>Feature</th>
<th>Extended DHCP Local Server</th>
<th>Traditional DHCP Local Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local address pools</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External, centrally-managed address pools</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Local configuration</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External configuration using information from address-assignment pools or RADIUS servers</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Dynamic-profile attachment</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>IPv6 client support</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Default minimum client configuration</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.
NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the **clear dhcp server binding** command before you delete the DHCP server configuration.

This overview covers:

**Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools**

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber’s computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

**Providing DHCP Client Configuration Information**

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP
application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool (such as, DNS server address), the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you might need to configure the local address-assignment pool to provide the configuration information, such as DNS server, for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 47 on page 721 lists the information that RADIUS might include in the authentication grant. See RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 47: Information in Authentication Grant

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS attribute 8</td>
<td>Framed-IP-Address</td>
<td>Client IP address</td>
</tr>
<tr>
<td>RADIUS attribute 9</td>
<td>Framed-IP-Netmask</td>
<td>Subnet mask for client IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(DHCP option 1)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-4</td>
<td>Primary-DNS</td>
<td>Primary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-5</td>
<td>Secondary-DNS</td>
<td>Secondary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-6</td>
<td>Primary-WINS</td>
<td>Primary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-7</td>
<td>Secondary-WINS</td>
<td>Secondary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>RADIUS attribute 27</td>
<td>Session-Timeout</td>
<td>Lease time</td>
</tr>
<tr>
<td>RADIUS attribute 88</td>
<td>Framed-Pool</td>
<td>Address assignment pool name</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-109</td>
<td>DHCP-Guided-Relay-Server</td>
<td>DHCP relay server</td>
</tr>
</tbody>
</table>
**Minimal Configuration for Clients**

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client’s subnet. This statement is the equivalent of DHCP option 3.

- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.

- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

**DHCP Local Server and Address-Assignment Pools**

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in external address-assignment pools (external to the DHCP local server). The external address-assignment pools are managed by the `authd` process, independently of the DHCP local server, and can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

**NOTE:** The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.
Configuring the Router as an Extended DHCP Local Server

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See Address-Assignment Pool Configuration Overview for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the dhcp-local-server statement at the [edit system services] hierarchy level:

```nconf
[edit system services]
dhcp-local-server {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
        }
    }
}
```
*domain-name* *domain-name-string*;
*logical-system-name*;
*mac-address*;
*option-60*;
*option-82* <circuit-id> <remote-id>;
*routing-instance-name*;
*user-prefix* *user-prefix-string*;
}
}

*group* *group-name* {
  *authentication* {
    *password* *password-string*;
    *username-include* {
      *circuit-type*;
      *delimiter* *delimiter-character*;
      *domain-name* *domain-name-string*;
      *logical-system-name*;
      *mac-address*;
      *option-60*;
      *option-82* <circuit-id> <remote-id>;
      *routing-instance-name*;
      *user-prefix* *user-prefix-string*;
    }
    }
  *
  } interface *interface-name* <upto upto-interface-name> <exclude>;
}

*pool-match-order* {
  *ip-address-first*;
  *option-82*;
}
}

You can also include these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* system services]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]
- [edit routing-instances *routing-instance-name* system services]

In addition, you can configure tracing for DHCP local server operations by including the *traceoptions* statement at the [edit system processes dhcp-service] hierarchy level:

```
[edit system processes]
  *traceoptions* {
```
Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server that will grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Extended DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.
The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See Address-Assignment Pool Configuration Overview for details about creating and using address-assignment pools.

**NOTE:** The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

### Methods Used by the Extended DHCP Local Server to Determine Which Address-Assignment Pool to Use

**IN THIS SECTION**

- Matching the Client IP Address to the Address-Assignment Pool | 727
- Matching Option 82 Information to Named Address Ranges | 727

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client. By default, the server matches the IP address in the client DHCP request to the address of the address-assignment pool.

The following sections describe the methods used by the DHCP local server to determine which address-assignment pool to use:
Matching the Client IP Address to the Address-Assignment Pool

In the default configuration, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

Matching Option 82 Information to Named Address Ranges

You can also configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool. To use the DHCP local server option 82 matching feature, you must ensure that the option-82 statement is included in the dhcp-attributes statement for the address-assignment pool.

NOTE: To enable the option 82 matching method, you must first specify the ip-address-first statement in the pool-match-order statement, and then specify the option-82 statement.

Default Options Provided by the Extended DHCP Server for the DHCP Client

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client’s subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.
Using External AAA Authentication Services to Authenticate DHCP Clients

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

*NOTE:* This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the `authentication-server` statement at the `[edit access profile profile-name]` hierarchy level.

Tasks for configuring External AAA authentication services are:

1. **Configuring Authentication Support for an Extended DHCP Application** | 728
2. **Grouping Interfaces with Common DHCP Configurations** | 730
3. **Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service** | 731
4. **Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service** | 731

**Configuring Authentication Support for an Extended DHCP Application**

To configure authentication support for an extended DHCP application, include the `authentication` statement at these hierarchy levels. You can configure either global authentication support or group-specific support.

You must configure the `username-include` statement to enable the use of authentication. The `password` statement is not required and does not cause DHCP to use authentication if the `username-include` statement is not included.

Extended DHCP local server hierarchies:

- `[edit system services dhcp-local-server]`
- `[edit system services dhcp-local-server group group-name]`
Extended DHCP relay agent hierarchies:

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```
Grouping Interfaces with Common DHCP Configurations

The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

To configure an interface group, use the `group` statement.

```
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    interface interface-name <upto upto-interface-name> <exclude>;
}
```

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface interface-name` statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

```
group boston {
    interface 192.168.10.1;
    interface 192.168.15.5;
}
```

You can use the `upto` option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
    interface 192.168.10.1 upto 192.168.10.255;
```
You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```lua
group paris {
    interface 192.168.100.1 exclude;
    interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

### Configuring Passwords for Usernames the DHCP Application Presents to the External AAA Authentication Service

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username, use the `password` statement. For example:

```lua
authentication {
    password myPassword1234;
}
```

### Creating Unique Usernames the Extended DHCP Application Passes to the External AAA Authentication Service

You can configure the extended DHCP application to include additional fields in the username passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.

#### NOTE:
No authentication is performed if you do not include a username in the authentication configuration; however, the IP address is provided by the local pool if it is configured.

To configure unique usernames, use the `username-include` statement. You can include any or all of the additional statements.

```lua
authentication [
    username-include [
        circuit-type;
    ]
]
The following list describes the attributes that can be included as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as string. The router adds the @ delimiter to the username.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of format **xxxx.xxxx.xxxx**.
- **option-60**—The portion of the option 60 payload that follows the length field.
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload.
  - **circuit-id**—The payload of the agent circuit ID suboption.
  - **remote-id**—The payload of the Agent Remote ID suboption.
  - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
  - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter. The default delimiter is a period (.). You can specify a different delimiter; however, the semicolon character (;) is not allowed.
The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
  username-include {
    circuit-type;
    domain-name isp55.com;
    mac-address;
    user-prefix wallybrown;
  }
}
```

The resulting unique username is:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

## Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.
When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following list shows the information that RADIUS might include in the authentication grant. See RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

- Client IP address—RADIUS attribute 8, Framed-IP-Address
- Subnet mask for client IP address (DHCP option 1)—RADIUS attribute 9, Framed-IP-Netmask
- Primary domain server (DHCP option 6)—VSA 26-4, Primary-DNS
- Secondary domain server (DHCP option 6)—VSA 26-5 Secondary-DNS
- Primary WINS server (DHCP option 44)—VSA 26-6, Primary-WINS
- Secondary WINS server (DHCP option 44)—VSA 26-7, Secondary-WINS
- Address assignment pool name—RADIUS attribute 88, Framed-Pool
- Lease time—RADIUS attribute 27, Session-Timeout
- DHCP relay server—VSA 26-109, DHCP-Guided-Relay-Server

Example: Configuring the Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

This example creates the server group named group_one, and specifies that the DHCP local server is enabled on interface fe-0/0/2.0 within the group. The DHCP local server uses the default pool match configuration of ip-address-first.

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```
Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        ip-address-first:
        option-82:
    }
}
```

Tracing Extended DHCP Local Server Operations

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are traced. If you include the `traceoptions` statement at the `[edit system processes dhcp-service]` hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called `jdhcpd` located in the `/var/log` directory.
- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and so on, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten. For more information about how log files are created, see the `Junos System Log Messages Reference`.
- Log files can be accessed only by the user who configures the tracing operation.
NOTE: In software releases earlier than Junos OS 11.4, you configured tracing statements at the
[edit system services dhcp-local-server] and [edit forwarding-options dhcp-relay] hierarchy levels. Starting in Junos OS Release 11.4, these statements have been deprecated and hidden in favor of a new statement at the [edit system processes dhcp-service] hierarchy level. The deprecated statements may be removed from a future release; we recommend that you transition to the new statement.

To trace DHCP local server operations, include the traceoptions statement at the [edit system processes dhcp-service] hierarchy level:

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable | no-world-readable >;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

The following topics describe the tracing operation configuration statements:

1. Configuring the Filename of the Extended DHCP Local Server Processes Log | 736
2. Configuring the Number and Size of Extended DHCP Local Server Processes Log Files | 736
3. Configuring Access to the Log File | 737
4. Configuring a Regular Expression for Lines to Be Logged | 737
5. Configuring Trace Option Flags | 738

Configuring the Filename of the Extended DHCP Local Server Processes Log

By default, the name of the file that records trace output is jdhcpd. You can specify a different name by including the file statement at the [edit system processes dhcp-service traceoptions] hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename;
```

Configuring the Number and Size of Extended DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed jdhcpd.0, then jdhcpd.1, and so on, until there are three trace files. Then the oldest trace file (jdhcpd.2) is overwritten.
You can configure the limits on the number and size of trace files by including the following statements at the [edit system processes dhcp-service traceoptions] hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (jdhcpd) reaches 2 MB, jdhcpd is renamed jdhcpd.0, and a new file called jdhcpd is created. When the new jdhcpd reaches 2 MB, jdhcpd.0 is renamed jdhcpd.1 and filename is renamed jdhcpd.0. This process repeats until there are 20 trace files. Then the oldest file (jdhcpd.19) is overwritten by the newest file (jdhcpd.0).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the file world-readable statement at the [edit system processes dhcp-service traceoptions] hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the file no-world-readable statement at the [edit system processes dhcp-service traceoptions] hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the match statement at the [edit system processes dhcp-service traceoptions] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes dhcp-service traceoptions]
file filename match regex;
```
Configuring Trace Option Flags

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the [edit system processes dhcp-service traceoptions] hierarchy level:

```plaintext
[edit system processes dhcp-service traceoptions]
flag flag;
```

You can configure the following tracing flags:

- **all**—Trace all operations.
- **auth**—Trace authentication operations.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **packet**—Trace packet decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpdp**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

RELATED DOCUMENTATION

- Extended DHCP Local Server on Switching Devices | 774
Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the `relay-option-82` statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

- **Agent Circuit ID** (suboption 1)—An ASCII string that identifies the interface on which the client DHCP packet is received.

  NOTE: If `relay-option-82` is configured, but none of the attributes under `relay-option-82` (that is, `circuit-id | remote-id | server-id-override`) are explicitly configured, then the default behavior is for the circuit-id (that is, suboption 1) to always be included in the option-82 value. This is true whether or not the `vendor-specific` attribute under `relay-option-82` is configured.

- **Agent Remote ID** (suboption 2)—An ASCII string assigned by the DHCP relay agent that securely identifies the client.

You can configure the option 82 support globally or for a named group of interfaces.

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the `delete relay-option-82` statement.
NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See DHCPv6 Relay Agent Options.

The following sections describe the option 82 operations you can configure:

**Configuring Option 82 Information**

You use the `relay-option-82` statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the `circuit-id` statement to include the Agent Circuit ID (suboption 1) in the packets, or the `remote-id` statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the `circuit-id` or `remote-id` statement without including any of the optional `prefix`, `use-interface-description`, `use-vlan-id`, `include-irb-and-l2`, or `no-vlan-interface-name` statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

  (fe | ge)-fpc/pic/port.subunit

  **NOTE:** For remote systems, the `subunit` is required and is used to differentiate an interface.

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

  (fe | ge)-fpc/pic/port:vlan-id

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:
NOTE: Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-fpc/pic/port.subunit:bridge-domain-name

- IRB interfaces that use VLANs:

  (fe | ge)-fpc/pic/port.subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the include-irb-and-l2 statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

  (fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the no-vlan-interface-name statement. The format is as follows:

  irb.subunit
To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.

   - To insert the Agent Circuit ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set circuit-id
     ```

   - To insert the Agent Remote ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set remote-id
     ```

   - To insert both, configure both set commands.

3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.

   See Including a Prefix in DHCP Options.

4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.

   See Including a Textual Description in DHCP Options.

---

**Overriding Option 82 Information**

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the option 82 information in DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-option-82
```

### Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the `host-name`, `logical-system-name`, and `routing-instance-name` options. The DHCP relay agent obtains the values for the `host-name`, `logical-system-name`, and `routing-instance-name` as follows:

- If you include the `host-name` option, the DHCP relay agent uses the hostname of the device configured with the `host-name` statement at the `[edit system]` hierarchy level.
- If you include the `logical-system-name` option, the DHCP relay agent uses the logical system name configured with the `logical-system` statement at the `[edit logical-system]` hierarchy level.
- If you include the `routing-instance-name` option, the DHCP relay agent uses the routing instance name configured with the `routing-instance` statement at the `[edit routing-instances]` hierarchy level or at the `[edit logical-system logical-system-name routing-instances]` hierarchy level.
If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the DHCP option information when you specify the prefix statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  hostname:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  ```
  host-name/logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
  ```

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the `vlan-id` value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.
2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.
   - To configure the Agent Circuit ID:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit circuit-id
   ```

   - To configure the Agent Remote ID:

   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit remote-id
   ```

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.
   - To include the prefix with the Agent Circuit ID:

   ```
   [edit forwarding-options dhcp-relay relay-option-82 circuit-id]
   user@host# set prefix host-name logical-system-name
   ```

   - To include the prefix with the Agent Remote ID:

   ```
   [edit forwarding-options dhcp-relay relay-option-82 remote-id]
   user@host# set prefix host-name logical-system-name
   ```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit dhcpv6
   ```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.
   - To configure option 18:

   ```
   [edit forwarding-options dhcp-relay dhcpv6]
   user@host# edit relay-agent-interface-id
   ```
To configure option 37:

```plaintext
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

- To include the prefix with option 18:

```plaintext
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

- To include the prefix with option 37:

```plaintext
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

### Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the `description` statement at the `[edit interfaces interface-name]` hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.
NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit circuit-id
   ```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

   ```
   [edit forwarding-options dhcp-relay relay-option-82 circuit-id]
   user@host# set use-interface-description device
   ```

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit dhcpv6
   ```
2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

- To include the textual description in option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description device
```

- To include the textual description in option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description device
```

SEE ALSO

- Configuring Interface Description
CHAPTER

DHCP for Switches

DHCP for Switches | 751
Extended DHCP Local Server | 774
DHCPv6 Local Server | 786
Extended DHCP Relay Agent | 791
DHCP Relay Agent Information Option (Option 82) | 810
DHCP Relay Proxy | 825
DHCPv6 Relay Agent | 828
Managing DHCP Services on Switches | 832
Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers | 849
Grouping Interfaces and Applying a Common DHCP Configuration to the Group | 853
Connectivity Liveness Detection in the DHCP Access Network | 858
Securing DHCP Messages Sent Between DHCP Clients and Servers in Different VRFs | 883
Assigning IP Addresses for DHCP | 889
A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A switch acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. You can configure a switch either as a DHCP server or as a DHCP relay server, but not both. For more information, read this topic.

**Understanding DHCP Services for Switches**

**IN THIS SECTION**
- DHCP Client/Server Model | 752
- Using DHCP | 752
- DHCP Relay Servers and DHCP Servers | 753
- Legacy DHCP and Extended DHCP for Server Versions | 753
- Configuring DHCP on a Switch | 754
- How DHCP Works | 754
A Dynamic Host Configuration Protocol (DHCP) server on a switch can provide many valuable TCP/IP network services. For example, DHCP can dynamically allocate the four required IP parameters to each computer on the LAN: IP address, network mask, switch address, and name server address. Additionally, DHCP on the switch can automatically upgrade software on client systems.

This topic describes:

**DHCP Client/Server Model**

DHCP IP address allocation works on a client/server model in which the server, in this case a switch, assigns the client reusable IP information from an address pool. A DHCP client might receive offer messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 38 on page 752.

Figure 38: DHCP Client/Server Model

**Using DHCP**

DHCP automates network-parameter assignment to network devices. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.

DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup, which means that you do not have to manually create and maintain IP address assignments for clients. In addition, when you use DHCP to manage a pool of IP addresses among hosts, you reduce the number of IP addresses needed on the network. DHCP does this by leasing an IP address to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses. DHCP also provides a central database of devices that are connected to the network and eliminates duplicate resource assignments. In addition to IP addresses for clients, DHCP provides other configuration information, particularly the IP addresses of local caching Domain Name System (DNS) resolvers, network boot servers, or other service hosts.
Another valuable DHCP feature is automatic software download for installation of software packages on switches. DHCP clients configured for automatic software download receive messages as part of the DHCP message exchange process—when the software package name in the DHCP server message is different from that of the software package that booted the DHCP client switch, the new software is downloaded and installed. See *Upgrading Software by Using Automatic Software Download for Switches*.

**DHCP Relay Servers and DHCP Servers**

You can configure a switch either as a DHCP server or as a DHCP relay server, but not both. Whereas a DHCP server replies to a client with an IP address, a DHCP relay server relays DHCP messages to and from the configured DHCP server, even if the client and server are on different IP networks.

Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

**Legacy DHCP and Extended DHCP for Server Versions**

Two versions of both DHCP server and DHCP relay agent are available on EX Series, QFX Series, and OCX Series switches. The original legacy DHCP server and legacy DHCP relay agent can be used in the same network as the extended DHCP servers and extended DHCP relay agent—extended DHCP is also referred to as virtual router (VR) aware DHCP.

You cannot configure legacy DHCP and extended DHCP versions on the same switch. Because the newer extended DHCP server version has more features, we recommend that you configure the extended DHCP server if it is supported by the switch.

The extended DHCP server version has the following added features:

- Graceful Routing Engine switchover (GRES), which provides mirroring support for clients.
- Virtual routing and forwarding (VRF), which allows multiple instances of a routing table to simultaneously coexist on the same switch. For details, see *Understanding Virtual Routing Instances on EX Series Switches*.

**NOTE:** Legacy DHCP supports the circuit ID and the remote ID fields for the relay agent option (option 82). Extended DHCP for the relay agent option supports only circuit ID. See *EX Series Switch Software Features Overview* for a list of switches that support extended DHCP (VR-aware DHCP).

Legacy DHCP and extended DHCP servers can be configured at the hierarchy levels shown in *Table 48 on page 754*:
### Configuring DHCP on a Switch

A DHCP configuration consists of two parts: the configuration for a DHCP server and the configuration for DHCP clients. The DHCP server configuration is simple if you accept the default configurations.

When you configure a legacy DHCP server, you only need to define the DHCP server name and the interface on the switch. You can use the default configuration for the rest of the settings. When you configure an extended DHCP server, you need to only define a DHCP pool, indicate IP addresses for the pool, and create a server group. You can use the default configuration for the rest of the settings.

For directions for configuring either a legacy DHCP server or an extended DHCP server, see “Configuring a DHCP Server on Switches (CLI Procedure)” on page 759.

To configure a DHCP client, set the client’s DHCP interface address in the \[edit interfaces interface-name unit 0 family inet dhcp\] hierarchy. For directions for configuring a DHCP client on a switch, see “Configuring a DHCP Client (CLI Procedure)” on page 762.

### How DHCP Works

DHCP consists of a four-step transfer process beginning with a broadcast DHCP discovery message from the client. As the second step, the client receives a DHCP offer message from the server. This message includes the IP address and mask, and some other specific parameters. The client then sends a DHCP request message to accept the IP address and other parameters that it received from the server in the previous step. The DHCP server sends a DHCP response message and removes the now-allocated address from the DHCP address pool. See Figure 39 on page 755.

---

**Table 48: Legacy DHCP and Extended DHCP Server Hierarchy Levels**

<table>
<thead>
<tr>
<th>DHCP Service</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP server</td>
<td>edit system services dhcp-local-server</td>
</tr>
<tr>
<td>Extended DHCP address pool</td>
<td>edit access address-assignment pool</td>
</tr>
<tr>
<td>Legacy DHCP server</td>
<td>edit system services dhcp</td>
</tr>
<tr>
<td>Legacy DHCP relay</td>
<td>edit forwarding-options helpers bootp</td>
</tr>
<tr>
<td>Extended DHCP relay</td>
<td>edit forwarding-options dhcp-relay</td>
</tr>
<tr>
<td>Legacy DHCP address pool</td>
<td>edit system services dhcp pool</td>
</tr>
</tbody>
</table>
NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

SEE ALSO

Upgrading Software by Using Automatic Software Download for Switches

Configuring a Switch as a DHCP Server (CLI Procedure)

NOTE: This topic applies to Junos OS for EX Series switches and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring a DHCP Server on Switches (CLI Procedure)" on page 759. For ELS details, see Using the Enhanced Layer 2 Software CLI.

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A switch acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the switch as a
local DHCP server using DHCP for IPv4 (DHCPv4). For information about DHCPv6 local server, see "DHCPv6 Local Server Overview" on page 787.

This topic describes the following task:

1. **Configuring the Switch as a Local DHCP Server**

**Configuring the Switch as a Local DHCP Server**

To configure a switch as a local DHCP server, you must configure a DHCP address pool and indicate IP addresses for the pool. The switch, operating as the DHCP server, dynamically distributes the IP addresses from this pool. The switch can dynamically assign additional configuration parameters, such as default gateway, to provide the client with information about the network.

Multiple address pools can be configured for a DHCP server. DHCP maintains the state information about all configured pools. Clients are assigned addresses from pools with subnets that match the interface on which the DHCPDISCOVER packet sent by the client is received on the server. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

You must ensure that you do not assign addresses that are already in use in the network to the address pools. The DHCP server does not check whether the addresses are already in use in the network before it assigns them to clients.

1. Configure a Layer 3 interface with an IP address on which the DHCP server will be reachable:

   ```
   [edit]
   user@switch# set interfaces interface-name unit unit-number family family address address/prefix-length
   user@switch# set vlans vlan-name vlan-id vlan-id
   user@switch# set vlans vlan-name l3-interface irb-name
   user@switch# set interfaces irb-name family family address address/prefix-length
   ```

   For example:

   ```
   [edit]
   user@switch# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
   user@switch# set vlans server vlan-id 301
   user@switch# set vlans server l3-interface irb.301
   user@switch# set interfaces irb.301 family inet address 192.0.2.2/24
   ```

2. Configure the DHCP server for the Layer 3 interface:

   ```
   [edit]
   user@switch# set system services dhcp-local-server group-name interface interface-name
   ```
For example:

```
[edit]
user@switch# set system services dhcp-local-server group server1 interface ge-0/0/1
user@switch# set system services dhcp-local-server group server1 interface irb.301
```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]
user@switch# set access address-assignment pool pool-name family family network address/prefix-length
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet network 198.51.100.0/24
```

4. (Optional) Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range:

```
[edit]
user@switch# set access address-assignment pool pool-name family family range range-name low low-IP-address
user@switch# set access address-assignment pool pool-name family family range range-name high high-IP-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet range range1 low 198.51.100.1
user@switch# set access address-assignment pool pool1 family inet range range1 high 198.51.100.2
```

5. (Optional) Configure one or more routers as the default gateway on the client’s subnet:

```
[edit]
user@switch# set access address-assignment pool pool-name family family dhcp-attributes router gateway-ip-address
```
For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes router 198.1.1.254
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@switch# set access address-assignment pool pool-name family family dhcp-attributes server-identifier ip-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes server-identifier 198.51.100.254
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease:

```
[edit]
user@switch# set access address-assignment pool pool-name family family dhcp-attributes maximum-lease-time seconds
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes maximum-lease-time 43,200
```

8. (Optional) Specify user-defined options to be included in DHCP packets:

```
[edit]
user@switch# set access address-assignment pool pool-name family family dhcp-attributes option option-id-number option-type option-value
```

For example:

```
[edit]
```
Configuring a DHCP Server on Switches (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see “Configuring a Switch as a DHCP Server (CLI Procedure)” on page 755. For ELS details, see Using the Enhanced Layer 2 Software CLI.

A Dynamic Host Configuration Protocol (DHCP) server can provide two valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients and it can also deliver software upgrades to clients.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the DHCP server. For information about reconfiguring a DHCP client, see “Configuring a DHCP Client (CLI Procedure)” on page 762.

You can configure either of two versions of a DHCP server on a switch— the extended server version or the legacy server version. We recommend that you configure the extended server unless you need to keep your DHCP server configuration backward-compatible with the legacy server version.

This topic includes the following tasks:

1. Configuring an Extended DHCP Server on a Switch  |  759
2. Configuring a Legacy DHCP Server on a Switch (CLI Procedure)  |  761

Configuring an Extended DHCP Server on a Switch

To configure an extended DHCP server, you must configure a DHCP pool, indicate IP addresses for the pool, and create a server group. Additional configurations are optional.

Do not assign addresses that are already in use in the network to address pools. The extended DHCP server does not check whether addresses are already in use before it assigns them to clients.

1. Create an address pool for DHCP IP addresses:
2. Configure an address-assignment pool that can be used by different client applications for DHCP dynamic assignment:

```
user@switch# set access address-pool address-pool
```

3. Create a server group on the switch, providing a group name and an interface name for DHCP:

```
[edit access address-assignment]
user@switch# set pool address-pool-name
```

4. (Optional) Process the information protocol data units (PDUs):

```
[edit system services dhcp-local-server]
user@switch# set overrides process-inform
```

5. (Optional) Redefine the order of attribute matching for pool selection:

```
[edit system services dhcp-local-server]
user@switch# set pool-match-order ip-address-first
```

6. (Optional) Enable dynamic reconfiguration triggered by the DHCP extended server for all DHCP clients or only for the DHCP clients serviced by the specified group of interfaces:

```
[edit system services dhcp-local-server]
user@switch# set reconfigure
```

```
[edit system services dhcp-local-server group group-name]
user@switch# set reconfigure
```
Configuring a Legacy DHCP Server on a Switch (CLI Procedure)

To configure a legacy DHCP server, you must configure a pool of IP addresses for dynamic assignment. You only need to supply a series of network addresses. Additional configurations are optional.

1. Configure a pool of IP addresses for dynamic assignment:

   [edit system services dhcp]
   user@switch# set pool network-range

   **NOTE:** Step 2 through Step 15 are for assigning global values at the [edit system services dhcp] hierarchy level. You can also assign the same values to a specific pool by using those same commands at the [edit system services dhcp pool network-range] hierarchy level.

2. (Optional) Change the domain search list used to resolve hostnames:

   [edit system services dhcp]
   user@switch# set domain-search [ domain-list ]

3. (Optional) Change the domain name server (DNS) name that the DHCP server advertises to clients:

   [edit system services dhcp]
   user@switch# set name-server address

4. (Optional) Change the DHCP options:

   [edit system services dhcp]
   user@switch# set option id-number

5. (Optional) Change the devices advertised to clients:

   [edit system services dhcp]
   user@switch# set router address

6. (Optional) Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete the DHCP setup. This configuration step is equivalent to DHCP Option 66:
7. (Optional) Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. This configuration step is equivalent to DHCP Option 67:

```
[edit system services dhcp]
user@switch# set boot-file filename
```

8. (Optional) Change the SIP server:

```
[edit system services dhcp]
user@switch# set sip-server addresses-or-names
```

For more information, see “Configuring a DHCP SIP Server (CLI Procedure)” on page 764.

9. (Optional) Change the DHCP client's hardware address:

```
[edit system services dhcp]
user@switch# set static-binding mac-address
```

10. (Optional) Change the NetBIOS name server:

```
[edit system services dhcp]
user@switch# set wins-server address
```

---

**Configuring a DHCP Client (CLI Procedure)**

A Dynamic Host Configuration Protocol (DHCP) server can provide many valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients, and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see
"Configuring a DHCP Server on Switches (CLI Procedure)" on page 759 or "Configuring a Switch as a DHCP Server (CLI Procedure)" on page 755.

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

```
[edit]
user@switch# set interfaces interface-name unit number family inet dhcp
configuration-statement
```

**NOTE:** Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

The options that you can configure are listed in Table 49 on page 763. Replace the variable `configuration-statement` with one or more of the statements listed in this table. If you do not explicitly configure these options, the switch uses default values for them.

Table 49: DHCP Client Settings

<table>
<thead>
<tr>
<th>Configuration Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>client-identifier</strong></td>
<td>Unique client ID—By default this consists of the hardware type (01 for Ethernet) and the MAC address (a.b.c.d). For this example, the value would be 01abcd.</td>
</tr>
<tr>
<td><strong>lease-time</strong></td>
<td>Time in seconds that a client holds the lease for an IP address assigned by a DHCP server. If a client does not request a specific lease time, then the server sends the default lease time. The default lease time on a Junos OS DHCP server is 1 day.</td>
</tr>
<tr>
<td><strong>retransmission-attempt</strong></td>
<td>Number of times the client attempts to retransmit a DHCP packet.</td>
</tr>
<tr>
<td><strong>retransmission-interval</strong></td>
<td>Time between transmission attempts.</td>
</tr>
<tr>
<td><strong>server-address</strong></td>
<td>IP address of the server that the client queries for an IP address.</td>
</tr>
<tr>
<td><strong>update-server</strong></td>
<td>TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch are propagated.</td>
</tr>
</tbody>
</table>
### Configuring a DHCP SIP Server (CLI Procedure)

You can use the `sip-server` statement on the EX Series switch to configure option 120 on a DHCP server. The DHCP server sends configured option values—Session Initiation Protocol (SIP) server addresses or names—to DHCP clients when they request them. Previously, you were only allowed to specify a SIP server by address using `[edit system services dhcp option 120]`. You specify either an IPv4 address or a fully qualified domain name to be used by SIP clients to locate a SIP server. You cannot specify both an address and name in the same statement.

To configure a SIP server using the `address` option:

```
[edit system services dhcp]
user@switch# set sip-server address
```

For example, to configure one address:

```
[edit system services dhcp]
user@switch set sip-server 192.168.0.11
```

To configure a SIP server using the `name` option:

```
[edit system services dhcp]
user@switch# set sip-server name
```

For example, to configure a name:

```
[edit system services dhcp]
user@switch set sip-server abc.example.com
```
DHCP and BOOTP Relay Overview

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

You can configure the switch to use the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent. For information on configuring this option, see the `source-address-giaddr` configuration statement.

You can also use smart DHCP relay, which enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure a Layer 3 interface, Layer 3 subinterface, or IRB interface with multiple IP addresses and configure that interface to be a relay agent.

**NOTE:** Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.

Configuring DHCP and BOOTP

You can configure a switch to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server or DHCP relay agent. When a switch is a relay agent, if a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

**NOTE:** This task uses the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring DHCP and BOOTP Relay" on page 766. For ELS details, see *Using the Enhanced Layer 2 Software CLI*. 
To configure a switch to be a server, use the `dhcp-local-server` statement. To configure a switch to be a relay agent, use the `dhcp-relay` statement.

If you want to enable BOOTP support when the switch is configured to be a DHCP server, enter the following statement:

```
[edit system services dhcp-local-server]
user@switch# set overrides bootp-support
```

If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides bootp-support
```

### Configuring DHCP and BOOTP Relay

**IN THIS SECTION**

- Configuring a DHCP and BOOTP Relay Agent | 767
- Configuring DHCP Smart Relay | 768

You can configure the QFX Series to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that if a locally attached host can issue a DHCP or BOOTP request as a broadcast message and the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

**NOTE:** This task uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see “Configuring DHCP and BOOTP” on page 765. For ELS details, see Using the Enhanced Layer 2 Software CLI.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which allows you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent using the primary gateway address, the switch can resend the requests via the alternative
gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 logical interface with multiple IP addresses and configure that interface to be a relay agent.

Configuring a DHCP and BOOTP Relay Agent

To configure a switch to act as a DHCP and BOOTP relay agent, include the `bootp` statement at the `[edit forwarding-options helpers]` hierarchy level:

```plaintext
[edit forwarding-options helpers]
bootp {
    apply-secondary-as-giaddr text-description;
    client-response-ttl number;
    description text-description;
    interface (interface-name | interface-group) {
        client-response-ttl number;
        description text-description;
        maximum-hop-count number;
        minimum-wait-time seconds;
        no-listen;
        server address
        apply-secondary-as-giaddr
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    relay-agent-option;
    server server-identifier
}
```

To include a description of the BOOTP service, DHCP service, or interface, use the `description` statement.

To configure a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the `interface` statement.

To stop packets from being forwarded, include the `no-listen` statement.

To set the maximum allowed number in the hops field of the BOOTP message, include the `maximum-hop-count` statement. BOOTP messages that have a larger number in the hops field than the maximum allowed are not forwarded. If you omit the `maximum-hop-count` statement, the default maximum number of hops is four.

To set the minimum allowed number of seconds in the `secs` field of the BOOTP message, include the `minimum-wait-time` statement. This setting configurations a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the `secs` field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).
To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the **server** statement. You can include multiple **server** statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the **client-response-ttl** statement.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options
helpers {
    bootp {
        description "dhcp relay agent global parameters";
        server 192.168.55.44;
        server 172.16.0.3 routing-instance c3;
        maximum-hop-count 10;
        minimum-wait-time 8;
        interface {
            xe-0/0/1 {
                description "use this info for this interface";
                server 10.10.10.10;
                server 192.168.14.14;
                maximum-hop-count 11;
                minimum-wait-time 3;
            }
            xe-0/0/2 {
                no-listen; ###ignore DHCPDISCOVER messages on this interface
            }
        }
    }
}
```

SEE ALSO

| **bootp** |

**Configuring DHCP Smart Relay**

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required
by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See Configuring IRB Interfaces on Switches and Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface for information about this approach.

- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See Understanding Layer 3 Logical Interfaces and Configuring a Layer 3 Logical Interface for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- set forwarding-options helpers bootp smart-relay-global: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.

- set forwarding-options helpers bootp interface interface-name smart-relay-agent: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

SEE ALSO

bootp

Graceful Routing Engine Switchover for DHCP

For EX Series switches, only extended DHCP local server maintains the state of active DHCP client leases. The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces. The extended DHCP local server also supports the use of Junos address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.
For MX Series routers, the extended DHCP local server and the DHCP relay agent applications both maintain the state of active DHCP client leases in the session database. The extended DHCP application can recover this state if the DHCP process fails or is manually restarted, thus preventing the loss of active DHCP clients in either of these circumstances. However, the state of active DHCP client leases is lost if a power failure occurs or if the kernel stops operating (for example, when the router is reloaded) on a single Routing Engine.

You can enable graceful switchover support on both EX Series switches and MX Series routers. To enable graceful switchover support for the extended DHCP local server or extended DHCP relay agent on a switch, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. To enable graceful Routing Engine switchover support on MX Series routers, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. You cannot disable graceful Routing Engine switchover support for the extended DHCP application when the router is configured to support graceful Routing Engine switchover.

For more information about using graceful Routing Engine switchover, see *Understanding Graceful Routing Engine Switchover*.

SEE ALSO

- Extended DHCP Local Server Overview | 718
- Extended DHCP Relay Agent Overview | 792
- Unified ISSU for High Availability in Subscriber Access Networks

**Centrally Configured Opaque DHCP Options**

**IN THIS SECTION**

- Data Flow for RADIUS-Sourced DHCP Options | 771
- Multiple VSA 26-55 Instances Configuration | 773
- DHCP Options That Cannot Be Centrally Configured | 773
Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management)

RADIUS-sourced DHCP options are also considered to be opaque, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router’s (switch’s) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

**NOTE:** You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.
Data Flow for RADIUS-Sourced DHCP Options

Figure 40 on page 772 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.

2. The DHCP local server initiates authentication with the Junos OS RADIUS client.

3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber’s (DHCP client’s) client-sourced DHCP options.

4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.

5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.

6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).
7. The subscriber (DHCP client) is configured with the DHCP options.

8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:
   • Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
   • Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
   • Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to be reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

**BEST PRACTICE:** For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

**NOTE:** If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the RO flags in the Subscriber Management RADIUS dictionary file. The R value indicates a multivalued reply attribute and the O value indicates an ordered attribute.

DHCP Options That Cannot Be Centrally Configured

Table 50 on page 774 shows the DHCP options that you must not centrally configure on the RADIUS server.
### Table 50: Unsupported Opaque DHCP Options

<table>
<thead>
<tr>
<th>DHCP Option</th>
<th>Option Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 0</td>
<td>Pad Option</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Option 51</td>
<td>IP Address Lease Time</td>
<td>Value is provided by RADIUS attribute 27 (Session-Timeout).</td>
</tr>
<tr>
<td>Option 52</td>
<td>Option Overload</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Option 53</td>
<td>DHCP Message Type</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 54</td>
<td>Server Identifier</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 55</td>
<td>Parameter Request List</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 255</td>
<td>End</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>-</td>
<td>DHCP magic cookie</td>
<td>Not supported.</td>
</tr>
</tbody>
</table>

**RELATED DOCUMENTATION**

- DHCP for Routing Devices | 693

**Extended DHCP Local Server**

**IN THIS SECTION**

- Extended DHCP Local Server Overview | 775
- Example: Minimum Extended DHCP Local Server Configuration | 780
- Disabling Automatic Binding of Stray DHCP Requests | 780
- Configuring a Token for DHCP Local Server Authentication | 782
- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) | 783
- Verifying and Managing DHCP Local Server Configuration | 785
The extended DHCP local server provides an IP address and other configuration information in response to a client request. Extended DHCP local server enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. For information, read this topic.

Extended DHCP Local Server Overview

IN THIS SECTION

- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 777
- Providing DHCP Client Configuration Information | 777
- Minimal Configuration for Clients | 779
- DHCP Local Server and Address-Assignment Pools | 779
Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. Table 46 on page 719 provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 51: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

<table>
<thead>
<tr>
<th>Feature</th>
<th>Extended DHCP Local Server</th>
<th>Traditional DHCP Local Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local address pools</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External, centrally-managed address pools</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Local configuration</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>External configuration using information from address-assignment pools or RADIUS servers</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Dynamic-profile attachment</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>IPv6 client support</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>Default minimum client configuration</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.
NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

This overview covers:

**Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools**

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- **On routers**—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- **On switches**—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

**Providing DHCP Client Configuration Information**

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP
application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool (such as, DNS server address), the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you might need to configure the local address-assignment pool to provide the configuration information, such as DNS server, for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 47 on page 721 lists the information that RADIUS might include in the authentication grant. See RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 52: Information in Authentication Grant

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS attribute 8</td>
<td>Framed-IP-Address</td>
<td>Client IP address</td>
</tr>
<tr>
<td>RADIUS attribute 9</td>
<td>Framed-IP-Netmask</td>
<td>Subnet mask for client IP address (DHCP option 1)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-4</td>
<td>Primary-DNS</td>
<td>Primary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-5</td>
<td>Secondary-DNS</td>
<td>Secondary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-6</td>
<td>Primary-WINS</td>
<td>Primary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-7</td>
<td>Secondary-WINS</td>
<td>Secondary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>RADIUS attribute 27</td>
<td>Session-Timeout</td>
<td>Lease time</td>
</tr>
<tr>
<td>RADIUS attribute 88</td>
<td>Framed-Pool</td>
<td>Address assignment pool name</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-109</td>
<td>DHCP-Guided-Relay-Server</td>
<td>DHCP relay server</td>
</tr>
</tbody>
</table>
Minimal Configuration for Clients

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client’s subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in external address-assignment pools (external to the DHCP local server). The external address-assignment pools are managed by the `authd` process, independently of the DHCP local server, and can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

**NOTE:** The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.
Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```

**NOTE:** The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates the server group named `group_one`, and specifies that the DHCP local server is enabled on interface `fe-0/0/2.0` within the group. The DHCP local server uses the default pool match configuration of `ip-address-first`.

**NOTE:** If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.
NOTE: Automatic binding of stray requests is enabled by default.

- To disable automatic binding behavior, include the `no-bind-on-request` statement when you configure DHCP overrides at the global, group, or interface level.

  ```
  [edit forwarding-options dhcp-relay overrides]
  user@host# set no-bind-on-request
  ```

- To override the default behavior for DHCPv6 relay agent, configure the override at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

  ```
  [edit forwarding-options dhcp-relay dhcpv6 overrides]
  user@host# set no-bind-on-request
  ```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

1. Specify the named group.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit group boston
   ```

2. Specify that you want to configure overrides.

   ```
   [edit forwarding-options dhcp-relay group boston]
   user@host# edit overrides
   ```

3. Disable automatic binding for the group.

   ```
   [edit forwarding-options dhcp-relay group boston overrides]
   user@host# set no-bind-on-request
   ```

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

   ```
   [edit forwarding-options dhcp-relay]
   ```
2. Specify the interface on which you want to disable automatic binding.

[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2

3. Specify that you want to configure overrides.

[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
user@host# edit overrides

4. Disable automatic binding on the interface.

[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request

---

**Configuring a Token for DHCP Local Server Authentication**

You can configure an authentication token to provide rudimentary protection against inadvertently instantiated DHCP servers. You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. If the service provider has previously configured the DHCP client with a token, then the client can compare that token against the newly received token. If the tokens do not match, the DHCP client discards the forcerenew message. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.
  
  For DHCPv4:

  [edit system services dhcp-local-server reconfigure]
  user@host# set token token-value
For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set token token-value
```

(Optional) For only a particular group of clients:

- Specify the token.

For DHCPv4:

```
[edit system services dhcp-local-server group group-name reconfigure]
user@host# set token token-value
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set token token-value
```

---

### Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)

You can configure an EX Series switch to act as an extended DHCP relay agent. This means that a locally attached host can issue a DHCP request as a broadcast message and the switch configured for DHCP relay relays the message to a specified DHCP server. Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Before you begin:

- Ensure that the switch can connect to the DHCP server.

To configure a switch to act as an extended DHCP relay agent server:

1. Create at least one DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

```
[edit forwarding-options dhcp-relay]
user@switch# set server-group server-group-name ip-address
```

2. Set the global active DHCP server group. The DHCP relay server relays DHCP client requests to the DHCP servers defined in the active server group:
3. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

```
[edit forwarding-options dhcp-relay]
user@switch# set active-server-group server-group-name
```

4. (Optional) Configure overrides of default DHCP relay behaviors, at the global level. See the override options in the `overrides` statement.

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides
```

5. (Optional) Configure DHCP relay to use the DHCP vendor class identifier option (option 60) in DHCP client packets, at the global level:

```
[edit forwarding-options dhcp-relay]
user@switch# set relay-option option-number 60
```

6. (Optional) Configure settings for a DHCP relay group that override the settings at the global level, using these statements:

```
[edit forwarding-options dhcp-relay group group-name]
user@switch# set active-server-group server-group-name
user@switch# set overrides
user@switch# set relay-option option-number 60
```

7. (Optional) Configure settings for a DHCP relay group interface that override the settings at the global and group levels, using these statements:

```
[edit forwarding-options dhcp-relay group group-name interface interface-name]
user@switch# exclude
user@switch# set overrides
user@switch# set trace
user@switch# set upto upto-interface-name
```
Verifying and Managing DHCP Local Server Configuration

Purpose
View or clear information about client address bindings and statistics for the extended DHCP local server.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Action
- To display the address bindings in the client table on the extended DHCP local server:
  
  `user@host> show dhcp server binding routing-instance customer routing instance`

- To display extended DHCP local server statistics:
  
  `user@host> show dhcp server statistics routing-instance customer routing instance`

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:
  
  `user@host> clear dhcp server binding routing-instance customer routing instance`

- To clear all extended DHCP local server statistics:
  
  `user@host> clear dhcp server statistics routing-instance customer routing instance`

RELATED DOCUMENTATION

- Extended DHCP Local Server On Routing Devices | 717
DHCPv6 Local Server

IN THIS SECTION

- DHCPv6 Local Server Overview | 787
- Specifying the Delegated Address Pool for IPv6 Prefix Assignment | 788
- Preventing Binding of Clients That Do Not Support Reconfigure Messages | 789
- Configuring DHCPv6 Rapid Commit (MX, EX) | 790
- Verifying and Managing DHCPv6 Local Server Configuration | 790

Junos OS device can act as a DHCPv6 server and allocates IP addresses to IPv6 clients. DHCPv6 server also delivers configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. For more information, read this topic.
DHCPv6 Local Server Overview

The DHCPv6 local server is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.

The DHCPv6 local server provides many of the same features as the DHCP local server, including:

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters
- AAA directed login
- Use of the IA_NA option to assign a specific address to a client

When a DHCPv6 client logs in, the DHCPv6 local server can optionally use the AAA service framework to interact with the RADIUS server. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters.

The client username, which uniquely identifies a subscriber or a DHCP client, must be present in the configuration in order for DHCPv6 local server to use RADIUS authentication.

You can configure DHCPv6 local server to communicate the following attributes to the AAA service framework and RADIUS at login time:

- Client username
- Client password

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 53 on page 787 to configure the client:

Table 53: RADIUS Attributes and VSAs for DHCPv6 Local Server

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>Lease time, in seconds. If not supplied, the lease does not expire</td>
</tr>
<tr>
<td>123</td>
<td>Delegated-IPv6-Prefix</td>
<td>Prefix that is delegated to the client</td>
</tr>
<tr>
<td>26-143</td>
<td>Max-Clients-Per-Interface</td>
<td>Maximum number of clients allowed per interface</td>
</tr>
</tbody>
</table>

To configure the extended DHCPv6 local server on the router (or switch), you include the `dhcpv6` statement at the [edit system services dhcp-local-server] hierarchy level.
You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name system services dhcp-local-server]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server]`

### Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

- On routers—Subscriber management uses the pool to assign IPv6 prefixes for subscribers. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.
- On switches—DHCP management uses the pool to assign IPv6 prefixes for DHCP clients. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

**NOTE:** You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value always takes precedence over the `delegated-address` statement.

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit overrides
   ```

2. Configure the delegated address pool.

   ```
   [edit system services dhcp-local-server dhcpv6 overrides]
   user@host# set delegated-pool paris-cable-12
   ```

### SEE ALSO

- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
- Extended DHCP Local Server Overview | 718
Preventing Binding of Clients That Do Not Support Reconfigure Messages

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.

To configure the DHCPv6 local server to bind only clients that support client-initiated reconfiguration:

• Specify strict reconfiguration.
  
  For all DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set strict
  ```

  For only a particular group of DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
  user@host# set strict
  ```

  The `show dhcpv6 server statistics` command displays a count of solicit messages that the server has discarded.

SEE ALSO

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview
- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients
Configuring DHCPv6 Rapid Commit (MX, EX)

You can configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the **overrides** options:

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit overrides
   ```

2. Enable rapid commit support:

   ```
   [edit system services dhcp-local-server dhcpv6 overrides]
   user@host# set rapid-commit
   ```

SEE ALSO

- Overriding the Default DHCP Local Server Configuration Settings Overview | 807

Verifying and Managing DHCPv6 Local Server Configuration

**Purpose**

View or clear information about client address bindings and statistics for the DHCPv6 local server.

**Action**

- To display the address bindings in the client table on the DHCPv6 local server:

  ```
  user@host> show dhcpv6 server binding
  ```
• To display DHCPv6 local server statistics:

```
user@host> show dhcpv6 server statistics
```

• To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server binding
```

• To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server statistics
```

RELATED DOCUMENTATION

- DHCP for Switches | 751
- Extended DHCP Local Server | 774

Extended DHCP Relay Agent

IN THIS SECTION

- Extended DHCP Relay Agent Overview | 792
- Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets | 795
- Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent | 795
- Replacing the DHCP Relay Request and Release Packet Source Address | 796
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings | 797
- Example: Minimum JDHCP Relay Agent Configuration | 802
- Verifying and Managing DHCP Relay Configuration | 802
- Overriding the Default DHCP Relay Configuration Settings | 803
- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
- Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally | 810
A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server. Extended DHCP local server enhances traditional DHCP relay agent operation.

Extended DHCP Relay Agent Overview

**IN THIS SECTION**

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers | 793
- DHCP Liveness Detection | 795
You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

**NOTE:** The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.

**NOTE:** The extended DHCP relay agent options configured with the `dhcp-relay` statement are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.

For information about the DHCP/BOOTP relay agent, see Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents.

You can also configure the extended DHCP relay agent to support IPv6 clients. See "DHCPv6 Relay Agent Overview" on page 829 for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level.

You can also include the `dhcp-relay` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name forwarding-options]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options]`
- `[edit routing-instances routing-instance-name forwarding-options]`

**Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers**
The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some differences in the details of usage.

On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. **The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.**

2. **The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.**

3. **In response to receiving the discover packet, each DHCP server sends an offer packet to the client.** The DHCP relay agent receives the offer packets and forwards them to the DHCP client.

4. **On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.**

5. **The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.**

6. **The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.**

7. **The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client’s configuration parameters.**

8. **The DHCP relay agent receives the ACK packet and forwards it to the client.**

9. **The DHCP client receives the ACK packet and stores the configuration information.**

10. **If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.**

11. **After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent “snoops” on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.**
DHCP Liveness Detection

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: DHCP liveness detection either globally or per DHCP group.

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set layer2-unicast-replies
   ```

Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.
To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the giaddr of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

---

Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]
user@host# set replace-ip-source-with giaddr
```
Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

IN THIS SECTION

- Requirements | 797
- Overview | 797
- Configuration | 798
- Verification | 800

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

Requirements

This example uses the following hardware and software components:

- MX Series 5G Universal Routing Platforms or EX Series Switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.
  
  See “Extended DHCP Relay Agent Overview” on page 792.

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.
  
  See “Grouping Interfaces with Common DHCP Configurations” on page 853.

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.

2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

**Configuration**

**IN THIS SECTION**

- Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings | 798
- Results | 799

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the [edit] hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal ffff local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

**Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings**

**Step-by-Step Procedure**

To configure DHCP relay selective processing:

1. Specify that you want to configure DHCP relay agent support.

   ```
   [edit forwarding-options]
   user@host# edit dhcp-relay
   ```

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

   ```
   [edit forwarding-options dhcp-relay]
   ```
3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group servergroup-15
```

6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal ffff local-server-group servergroup-east
```

**Results**

From configuration mode, confirm the results of your configuration by issuing the `show` statement at the `[edit forwarding-options]` hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  relay-option {
    option-number 60;
    equals {
      ascii video-gold {
        forward-only;
      }
    }
  }
}```
If you are done configuring the device, enter **commit** from configuration mode.

**Verification**

To verify the status of DHCP relay agent selective traffic processing, perform this task:

*Verifying the Status of DHCP Relay Agent Selective Traffic Processing*

**Purpose**

Verify the DHCP relay agent selective traffic processing status.

**Action**

Display statistics for DHCP relay agent.

```
user@host> show dhcp relay statistics
```

<table>
<thead>
<tr>
<th>Packets dropped:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
</tr>
<tr>
<td>30</td>
</tr>
</tbody>
</table>
Bad hardware address 1
Bad opcode 1
Bad options 3
Invalid server address 5
No available addresses 1
No interface match 2
No routing instance match 9
No valid local address 4
Packet too short 2
Read error 1
Send error 1
Option 60 1
Option 82 2

Messages received:
BOOTREQUEST 116
DHCPDECLINE 0
DHCPDISCOVER 11
DHCPINFORM 0
DHCPRELEASE 0
DHCPREQUEST 105

Messages sent:
BOOTREPLY 0
DHCPOFFER 2
DHCPACK 1
DHCPNAK 0
DHCPFORCERENEW 0

Packets forwarded:
Total 4
BOOTREQUEST 2
BOOTREPLY 2

Meaning
The Packets forwarded field in the show dhcp relay statistics command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of BOOTREQUEST and BOOTREPLY packets forwarded.
Example: Minimum JDHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
    server-group {
        test 203.0.113.21;
    }
    active-server-group test;
    group all {
        interface fe-0/0/2.0;
    }
}
```

**NOTE:** The interface type in this topic is just an example. The `fe-` interface type is not supported by EX Series switches.

This example creates a server group and an active server group named `test` with IP address 203.0.113.21. The DHCP relay agent configuration is applied to a group named `all`. Within this group, the DHCP relay agent is enabled on interface `fe-0/0/2.0`.

Verifying and Managing DHCP Relay Configuration

**Purpose**
View or clear address bindings or statistics for DHCP relay agent clients.

**Action**
- To display the address bindings for DHCP relay agent clients:

  ```
  user@host> show dhcp relay binding
  ```

- To display DHCP relay agent statistics:

  ```
  user@host> show dhcp relay statistics
  ```

- To clear the binding state of DHCP relay agent clients:
To clear all DHCP relay agent statistics:

```
user@host> clear dhcp relay binding
```

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp relay binding routing instance <routing-instance name>`
- `show dhcp relay statistics routing instance <routing-instance name>`
- `clear dhcp relay binding routing instance <routing-instance name>`
- `clear dhcp relay statistics routing instance <routing-instance name>`

**NOTE:** On all SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

**SEE ALSO**

- *Minimum DHCP Relay Agent Configuration*

### Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP relay configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP relay agent configuration options, include the `overrides` statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level.
- To override DHCP relay configuration options for a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level.
• To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the `edit forwarding-options dhcp-relay group group-name interface interface-name` hierarchy level.

• To configure overrides for DHCPv6 relay at the global level, group level, or per-interface, use the corresponding statements at the `edit forwarding-options dhcp-relay dhcpv6` hierarchy level.
To override default DHCP relay agent configuration settings:

1. (DHCPv4 and DHCPv6) Specify that you want to configure override options.
   - DHCPv4 overrides.
     Global override:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```
     Group-level override:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name overrides
     ```
     Per-interface override:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name interface interface-name overrides
     ```
   - DHCPv6 overrides.
     Global override:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```
     Group-level override:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name overrides
     ```
     Per-interface override:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name interface interface-name overrides
     ```

2. (DHCPv4 only) Enable DHCP relay proxy mode.
   See “Enabling DHCP Relay Proxy Mode” on page 828.

3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.
See “Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent” on page 795.

4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
   See “Replacing the DHCP Relay Request and Release Packet Source Address” on page 796.

5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.
   See “Overriding Option 82 Information” on page 742.

6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.
   See “Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets” on page 795.

7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.
   See “Enable Processing of Untrusted Packets So Option 82 Information Can Be Used” on page 822.

8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.
   See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 837.

9. (DHCPv4 only) Configure client auto logout.
   See “DHCP Auto Logout Overview” on page 822.

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.
    See Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent.

11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.
    See the delay-authentication.

12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.
    See “Sending Release Messages When Clients Are Deleted” on page 840.

13. (Optional) Specify that when the DHCP or DHCPv6 relay agent receives a Discover or Solicit message that has a client ID that matches the existing client entry, the relay agent deletes the existing client entry.
    See DHCP Behavior When Renegotiating While in Bound State.
14. (DHCPv6 only) Automatically log out existing client when new client solicits on same interface.
   See *Automatically Logging Out DHCPv6 Clients*.

15. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.
   See "Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally" on page 810.

16. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.
   See "Disabling Automatic Binding of Stray DHCP Requests" on page 780.

17. (DHCPv4 and DHCPv6) Assign a single-session DHCP dual-stack group to a specified group of
   subscribers. You must assign the group to both legs of the DHCP dual stack.
   See *Configuring Single-Session DHCP Dual-Stack Support*.

18. (Optional, DHCPv4 and DHCPv6) Specify that a short lease be sent to the client.
   See *Configuring DHCP Asymmetric Leasing*.

---

**Overriding the Default DHCP Local Server Configuration Settings Overview**

Subscriber management enables you to override certain default DHCP local server configuration settings. You can override the configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP local server configuration options, include the `overrides` statement and its subordinate statements at the `edit system services dhcp-local-server` hierarchy level.

- To override DHCP local server configuration options for a named group of interfaces, include the statements at the `edit system services dhcp-local-server group group-name` hierarchy level.

- To override DHCP local server configuration options for a specific interface within a named group of interfaces, include the statements at the `edit system services dhcp-local-server group group-name interface interface-name` hierarchy level.

- To configure overrides for DHCPv6 local server at the global level, group level, or per-interface, use the corresponding statements at the `edit system services dhcp-local-server dhcpv6` hierarchy level.
To override default DHCP local server configuration settings:

1. (DHCPv4 and DHCPv6) Specify that you want to configure override options.
   
   - **DHCPv4 overrides.**
     
     Global override:
     
     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```

     Group-level override:
     
     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name overrides
     ```

     Per-interface override:
     
     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name overrides interface interface-name
     ```

   - **DHCPv6 overrides.**
     
     Global override:
     
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit overrides
     ```

     Group level override:
     
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit group group-name overrides
     ```

     Per-interface override:
     
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit group group-name overrides interface interface-name
     ```

2. (Optional) Override the maximum number of DHCP clients allowed per interface.
   
   See "Specifying the Maximum Number of DHCP Clients Per Interface" on page 837.

3. (Optional) Configure DHCP client auto logout.
   
   See "Automatically Logging Out DHCP Clients" on page 824.
4. (Optional) Enable processing of information requests from clients.
   See "Enabling Processing of Client Information Requests" on page 839.

5. (Optional) Specify that DHCP NAK and FORCERENEW messages support option 82 information.
   See Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances.

6. (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.
   See Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation.

7. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.
   See "Configuring DHCPv6 Rapid Commit (MX, EX)" on page 790.

8. (Optional, DHCPv6 only) Specify that DHCPv6 local server return DNS server addresses as IA_NA or IA_PD suboptions rather than as a global DHCPv6 option.
   See Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment.

9. (Optional, DHCPv6 only) Automatically log out existing client when new client solicits on same interface.
   See Automatically Logging Out DHCPv6 Clients.

10. (Optional) Specify that when the DHCP or DHCPv6 local server receives a Discover or Solicit message that has a client ID that matches the existing client entry, the local server deletes the existing client entry.
    See DHCP Behavior When Renegotiating While in Bound State.

11. (Optional, DHCPv4 and DHCPv6) Specify that a short lease be sent to the client.
    See Configuring DHCP Asymmetric Leasing.

12. (Optional, DHCPv4 and DHCPv6) Specify DHCP attributes globally or for groups.
    See Configuring DHCP Attributes for All Clients or a Group of Clients.

13. Load balance traffic by allowing some local servers to respond to specific clients while preventing other local servers from responding immediately to these clients.
    See Delaying DHCP Offer and Advertise Responses to Load Balance DHCP Servers.
Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Disable the DHCP relay agent.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set disable-relay
```

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>DHCP for Switches</th>
<th>751</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP Local Server</td>
<td>774</td>
</tr>
</tbody>
</table>

DHCP Relay Agent Information Option (Option 82)

IN THIS SECTION

- Using DHCP Relay Agent Option 82 Information | 811
- How DHCP Relay Agent Uses Option 82 for Auto Logout | 820
- Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | 822
- DHCP Auto Logout Overview | 822
- Automatically Logging Out DHCP Clients | 824
The DHCP relay agent information option (option 82) enables you to include additional useful information in the client-originated DHCP packets that the DHCP relay forwards to a DHCP server. You can configure the option 82 support globally or for a named group of interfaces. For more information, read this topic.

Using DHCP Relay Agent Option 82 Information

Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the `relay-option-82` statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which the client DHCP packet is received.

  NOTE: If `relay-option-82` is configured, but none of the attributes under `relay-option-82` (that is, `circuit-id | remote-id | server-id-override`) are explicitly configured, then the default behavior is for the circuit-id (that is, suboption 1) to always be included in the option-82 value. This is true whether or not the `vendor-specific` attribute under `relay-option-82` is configured.

- Agent Remote ID (suboption 2)—An ASCII string assigned by the DHCP relay agent that securely identifies the client.
You can configure the option 82 support globally or for a named group of interfaces.

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the `delete relay-option-82` statement.

NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See *DHCPv6 Relay Agent Options*.

The following sections describe the option 82 operations you can configure:

### Configuring Option 82 Information

You use the `relay-option-82` statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the `circuit-id` statement to include the Agent Circuit ID (suboption 1) in the packets, or the `remote-id` statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the `circuit-id` or `remote-id` statement without including any of the optional `prefix`, `use-interface-description`, `use-vlan-id`, `include-irb-and-l2`, or `no-vlan-interface-name` statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

  \[(fe | ge)-fpc/pic/port.subunit\]

  NOTE: For remote systems, the `subunit` is required and is used to differentiate an interface.

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

  \[(fe | ge)-fpc/pic/port:vlan-id\]
For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:

```
(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

**NOTE:** Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  ```
  (fe | ge)-fpc/pic/port.subunit:bridge-domain-name
  ```

- IRB interfaces that use VLANs:

  ```
  (fe | ge)-fpc/pic/port.subunit:vlan-name
  ```

To include the IRB interface name with the Layer 2 interface name, configure the `include-irb-and-l2` statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  ```
  (fe | ge):-fpc/pic/port:bridge-domain-name+irb.subunit
  ```

- IRB interfaces that use VLANs:

  ```
  (fe | ge)-fpc/pic/port:vlan-name+irb.subunit
  ```

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the `no-vlan-interface-name` statement. The format is as follows:

```
irb.subunit
```
To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.

   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82

2. Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.
   • To insert the Agent Circuit ID:
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set circuit-id
   • To insert the Agent Remote ID:
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set remote-id
   • To insert both, configure both set commands.

3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.
   See Including a Prefix in DHCP Options.

4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.
   See Including a Textual Description in DHCP Options.

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

• If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.

• If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.
To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.

   [edit forwarding-options dhcp-relay]
   user@host# edit overrides

2. Specify that the option 82 information in DHCP packets is overwritten.

   [edit forwarding-options dhcp-relay overrides]
   user@host# set always-write-option-82

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the host-name, logical-system-name, and routing-instance-name options. The DHCP relay agent obtains the values for the host-name, logical-system-name, and routing-instance-name as follows:

- If you include the host-name option, the DHCP relay agent uses the hostname of the device configured with the host-name statement at the [edit system] hierarchy level.
- If you include the logical-system-name option, the DHCP relay agent uses the logical system name configured with the logical-system statement at the [edit logical-system] hierarchy level.
- If you include the routing-instance-name option, the DHCP relay agent uses the routing instance name configured with the routing-instance statement at the [edit routing-instances] hierarchy level or at the [edit logical-system logical-system-name routing-instances] hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).
The following examples show several possible formats for the DHCP option information when you specify the prefix statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  host-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  logical-system-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  
  
  
  
  host-name/logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id_vlan-id

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the vlan-id value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

   
   
   
   
   [edit forwarding-options dhcp-relay]
   
   user@host# edit relay-option-82
2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.
   • To configure the Agent Circuit ID:
     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# edit circuit-id
     ```
   • To configure the Agent Remote ID:
     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# edit remote-id
     ```

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.
   • To include the prefix with the Agent Circuit ID:
     ```
     [edit forwarding-options dhcp-relay relay-option-82 circuit-id]
     user@host# set prefix host-name logical-system-name
     ```
   • To include the prefix with the Agent Remote ID:
     ```
     [edit forwarding-options dhcp-relay relay-option-82 remote-id]
     user@host# set prefix host-name logical-system-name
     ```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit dhcpv6
   ```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.
   • To configure option 18:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit relay-agent-interface-id
     ```
   • To configure option 37:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     ```
3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

- To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

- To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

### Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the `description` statement at the `[edit interfaces interface-name]` hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.
NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit circuit-id
   ```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

   ```
   [edit forwarding-options dhcp-relay relay-option-82 circuit-id]
   user@host# set use-interface-description device
   ```

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit dhcpv6
   ```
2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

  \[ \text{[edit forwarding-options dhcp-relay dhcpv6]} \]
  \[ \text{user@host# edit relay-agent-interface-id} \]

- To configure option 37:

  \[ \text{[edit forwarding-options dhcp-relay dhcpv6]} \]
  \[ \text{user@host# edit relay-agent-remote-id} \]

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

- To include the textual description in option 18:

  \[ \text{[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]} \]
  \[ \text{user@host# set use-interface-description device} \]

- To include the textual description in option 37:

  \[ \text{[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]} \]
  \[ \text{user@host# set use-interface-description device} \]

SEE ALSO

- Configuring Interface Description

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 54 on page 821 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.
<table>
<thead>
<tr>
<th>DHCP Relay Configured with Option 82</th>
<th>Discover Packet Contains Option 82</th>
<th>Override &quot;trust-option-82&quot;</th>
<th>Override &quot;always-write-option-82&quot;</th>
<th>giaddr in non-snoop packet</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>No secondary search performed</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>–</td>
<td>–</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>–</td>
<td>Zero</td>
<td>Drop packet</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>–</td>
<td>Non-zero</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>Use configured option 82</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>–</td>
<td>Zero</td>
<td>Drop packet</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Non-zero</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Non-zero</td>
<td>Overwrite the configured option 82</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>–</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>–</td>
<td>Overwrite the configured option 82</td>
</tr>
</tbody>
</table>
Enable Processing of Untrusted Packets So Option 82 Information Can Be Used

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set trust-option-82
   ```

DHCP Auto Logout Overview

IN THIS SECTION

- Auto Logout Overview | 822
- How DHCP Identifies and Releases Clients | 823
- Option 60 and Option 82 Requirements | 824

This topic provides an introduction to the DHCP auto logout feature and includes the following sections:

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the address
pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

**How DHCP Identifies and Releases Clients**

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- **Incoming interface method**— DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.

  ![NOTE: The incoming interface method differs from the *overrides interface-client-limit* 1 statement, which retains the existing binding and rejects the newly connected client.](image)

- **Option 60 and option 82 method**— DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- **DHCP local server immediately releases the existing address.**
• DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client’s existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in "DHCP Relay Agent Option 82 Value for Auto Logout" on page 821.

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet from a client whose identity matches an existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
   • For DHCP local server:
• For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable auto logout and specify the secondary identification method you want to use when the primary identification method is unsuccessful.

• For example, to configure DHCP local server to use the incoming interface method:

```
[edit system services dhcp-local-server overrides]
user@host# set client-discover-match incoming-interface
```

• For example, to configure DHCP relay agent to use the option 60 and option 82 method:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set client-discover-match option60-and-option82
```

NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

RELATED DOCUMENTATION

| DHCP for Switches | 751 |

DHCP Relay Proxy

IN THIS SECTION

- DHCP Relay Proxy Overview | 826
- Enabling DHCP Relay Proxy Mode | 828
A DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers. The DHCP relay agent is configured on the router or switch, which operates between the DHCP client and one or more DHCP servers. For more information, read this topic.

**DHCP Relay Proxy Overview**

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

**NOTE:** You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

**Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers**

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.

2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.

3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
   a. Selects the first offer received as the offer to sent to the client
b. Replaces the DHCP server address with the address of the DHCP relay proxy

c. Forwards the offer to the DHCP client.

4. The DHCP client receives the offer from the DHCP relay proxy.

5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.

6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.

7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.

8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.

9. The DHCP client receives the ACK packet and stores the configuration information.

10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.

11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

**Benefits of Using DHCP Relay Proxy**

DHCP relay proxy provides the following benefits:

- **DHCP server isolation and DoS protection**—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.

- **Multiple lease offer selection**—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.

- **Support for both numbered and unnumbered Ethernet interfaces**—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.

- **Logical system support**—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.
Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

   [edit forwarding-options dhcp-relay]
   user@host# edit overrides

2. Enable DHCP relay proxy mode.

   [edit forwarding-options dhcp-relay overrides]
   user@host# set proxy-mode

RELATED DOCUMENTATION

DHCP for Switches | 751

DHCPv6 Relay Agent

IN THIS SECTION

- DHCPv6 Relay Agent Overview | 829
- Inserting DHCPv6 Interface-ID Option (Option 18) in DHCPv6 Packets | 830
- Verifying and Managing DHCPv6 Relay Configuration | 831

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCPv6 Relay Agent relays DHCP messages between DHCPv6 clients and DHCPv6 servers in an IPv6 network. For more information, read this topic.
DHCPv6 Relay Agent Overview

The DHCPv6 relay agent enhances the DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agents support an IPv4 network. DHCPv6 relay agents eliminate the necessity of having a DHCPv6 server on each physical network.

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

NOTE: The following DHCPv6 functionalities are not supported on ACX Series routers:

- Subscriber authentication for DHCPv6 relay agents
- DHCP snooping
- DHCPv6 client
- Liveness detection
- Dynamic profiles
- Option 37 support for remote ID insertion
- Bidirectional Forwarding Detection (BFD) for DHCPv6 relay
- DHCPv6 relay persistence on router reboot, crash, or power failure

The DHCPv6 relay agent is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the DHCP local server or DHCP relay agent.

To configure the DHCPv6 relay agent on the router (or switch), you include the `dhcpv6` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name forwarding-options dhcp-relay]`
• [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay]
• [edit routing-instances routing-instance-name forwarding-options dhcp-relay]

See DHCPv6 Monitoring and Management for commands specific to viewing and clearing DHCPv6 bindings and statistics.

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

• Prefix—Specify the prefix option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.

• Interface description—Specify the use-interface-description option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.

• Option 82 Agent Circuit ID suboption (suboption 1)—Specify the use-option-82 option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.
3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the **logical** interface description or the **device** interface description.

   ```
   [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
   user@host# set prefix prefix
   ```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

   ```
   [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
   user@host# set use-option-82
   ```

**SEE ALSO**

- *Including a Prefix in DHCP Options*
- *Including a Textual Description in DHCP Options*

### Verifying and Managing DHCPv6 Relay Configuration

**Purpose**

View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

**Action**

- To display the address bindings for extended DHCPv6 relay agent clients:

  ```
  user@host> show dhcpv6 relay binding
  ```

- To display extended DHCPv6 relay agent statistics:

  ```
  user@host> show dhcpv6 relay statistics
  ```

- To clear the binding state of DHCPv6 relay agent clients:
Junos OS allows you to perform different types of DHCP services such as attaching dynamic profiles, using external authentication services with DHCP, specifying maximum number of clients, managing client information request messages, dynamic reconfiguration of clients and so on. For more information, read this topic.
Using External AAA Authentication Services with DHCP

The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

NOTE: This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and responds as though it were requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the authentication-server statement at the [edit access profile profile-name] hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the username-include statement to enable the use of authentication. The password statement is not required and does not cause DHCP to use authentication if the username-include statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```
   - For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6]
     ```
For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit authentication
```

2. (Optional) Configure a password that authenticates the username to the external authentication service. See Configuring Passwords for Usernames.

3. (Optional) Configure optional features to create a unique username.

See “Creating Unique Usernames for DHCP Clients” on page 834.

---

**Creating Unique Usernames for DHCP Clients**

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers (DHCP clients).

**NOTE:** If you do not include a username in the authentication configuration, the router (or switch) does not perform authentication; however, the IP address is provided by the local pool if it is configured.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.

The following list describes the optional information that you can include as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example enet.
- **client-id**—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as a string. The router adds the @ delimiter to the username.
- **interface-description**—The description of the device (physical) interface or the logical interface.
- **interface-name**—The interface name, including the interface device and associated VLAN IDs.
• **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.

• **mac-address**—The client MAC address, in a string of the format `xxxx.xxxx.xxxx`.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

• Client DUID Type 1 or Type 3.

• Option 79 (client link-layer address), if present.

• The packet source address if the client is directly connected.

• The link local address.

• **option-60**—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)

• **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)

  • **circuit-id**—The payload of the Agent Circuit ID suboption.

  • **remote-id**—The payload of the Agent Remote ID suboption.

  • Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: `circuit-id[delimiter]remote-id`.

  • Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.

  **NOTE:** For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

• **relay-agent-interface-id**—The Interface-ID option (option 18). (DHCPv6 local server or DHCPv6 relay agent only)

• **relay-agent-remote-id**—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server or DHCPv6 relay agent only)

• **relay-agent-subscriber-id**—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server or DHCPv6 relay agent only)

• **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.

• **user-prefix**—A string indicating the user prefix.

• **vlan-tags**—The subscriber VLAN tags. Includes the outer VLAN tag and, if present, the inner VLAN tag. You can use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.
The router (switch) creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

For DHCP local server and DHCP relay agent:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
option-60@domain-name
```

For DHCPv6 local server:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
relay-agent-subscriber-id[delimiter]relay-agent-interface-id[delimiter]client-id@domain-name
```

To configure a unique username:

1. Specify that you want to configure authentication.
   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```
   - For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit authentication
     ```
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit authentication
     ```

**NOTE:** You can also configure authentication and usernames for groups at additional hierarchy levels. See authentication (DHCP Local Server) and authentication (DHCP Relay Agent).
2. Specify that you want to include optional information in the username. (DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support the **username-include** statement.)

   ```
   [edit system services dhcp-local-server authentication]
   user@host# set username-include
   ```

3. (Optional) Specify the optional information you want to include in the username. DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support the **username-include** statement.

   The following sample configuration produces this unique username:
   ```
   wallybrown.00:00:5e:00:53:ff.enet@example.com
   ```

   ```
   [edit system services dhcp-local-server authentication username-include]
   user@host# set username-include circuit-type
   user@host# set username-include domain-name example.com
   user@host# set username-include mac-address
   user@host# set username-include user-prefix wallybrown
   ```

---

**Specifying the Maximum Number of DHCP Clients Per Interface**

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

---

**NOTE:** The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the **interface-client-limit** statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.
• For DHCP local server:

  [edit system services dhcp-local-server]
  user@host# edit overrides

• For DHCPv6 local server:

  [edit system services dhcp-local-server dhcpv6]
  user@host# edit overrides

• For DHCP relay agent:

  [edit forwarding-options dhcp-relay]
  user@host# edit overrides

• For DHCPv6 relay agent:

  [edit forwarding-options dhcp-relay dhcpv6]
  user@host# edit overrides

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the `interface-client-limit` statement.)

  [edit system services dhcp-local-server overrides]
  user@host# set interface-client-limit number

NOTE: For DHCP local server and DHCP relay agent, you can use either the `interface-client-limit` statement or the `client-discover-match incoming-interface` statement to set a limit of one client per interface. The `interface-client-limit` statement with a value of 1 retains the existing client and rejects any new client connections. The `client-discover-match incoming-interface` statement deletes the existing client and allows a new client to connect.

### DHCP Local Server Handling of Client Information Request Messages

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP inform or DHCPv6 information-request message that indicates what information is desired. These message types can be collectively referred to as information request
messages. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients is typically configured with the dhcp-attributes statement for an address pool defined by the address-assignment pool pool-name statement at the [edit access] hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify the name of the pool from which the local server retrieves the requested configuration information for the client. If you do not do specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.

NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data can be used to select the pool from which the response information is taken. Additionally other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap exists between RADIUS attributes and local pool attributes, the RADIUS values are used instead of the local configuration data. If no RADIUS information is received from the underlying PPP interface, then the behavior is the same as described previously for non-PPP interfaces.

**Enabling Processing of Client Information Requests**

By default, DHCP local server and DHCPv6 local server do not respond to information request (DHCP inform and DHCPv6 information-request) messages from the client. You can enable DHCP local server and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The
messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See Configuring an Address-Assignment Pool Name and Addresses. For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address for details about how to configure the information sought by clients that send information request messages.

To enable processing of DHCP client information request messages:

1. Specify that you want to configure override options.
   
   - For DHCP local server:
     
     ```
     [edit system services dhcp-local-server overrides]
     user@host# set process-inform
     ```

   - For DHCPv6 local server:
     
     ```
     [edit system services dhcp-local-server dhcpv6 overrides]
     user@host# set process-inform
     ```

2. (Optional) Specify a pool name from which DHCP information is returned to the client.
   
   - For DHCP local server:
     
     ```
     [edit system services dhcp-local-server overrides process-inform]
     user@host# set pool pool-name
     ```

   - For DHCPv6 local server:
     
     ```
     [edit system services dhcp-local-server dhcpv6 overrides process-inform]
     user@host# set pool pool-name
     ```

---

**Sending Release Messages When Clients Are Deleted**

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.
NOTE: You must include the `send-release-on-delete` statement to configure DHCP relay and relay proxy to send the release message when the `client-discover-match` statement is included.

You can use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set send-release-on-delete
   ```

---

**Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients**

Dynamic reconfiguration of clients enables the extended DHCP local server to initiate a client update without waiting for the client to initiate a request.

**Default Client/Server Interaction**

Typically the DHCP client initiates all of the basic DHCP client/server interactions. The DHCP server sends information to a client only in response to a request from that client. This behavior does not enable a client to be quickly updated with its network address and configuration in the event of server changes:
NOTE: Technically, the DHCP client/server interactions are the same on routers and switches. However, the primary usage of this technology on the routers is for subscriber management. The switches are not used for subscriber management. Therefore, this topic provides two sample scenarios. The actions are the same, but the implementation details are different.

- On routers—Suppose a service provider restructures its addressing scheme or changes the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.

- On switches—Suppose you restructure the addressing scheme or change the server IP addresses that the DHCP server provides to clients. Without dynamic reconfiguration, the network typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, you can wait for users to notify you of the network failures and then instruct them to power cycle their equipment to reinitiate the connection. Neither of these actions is timely or convenient for users.

Dynamic Client/Server Interaction for DHCPv4

Dynamic reconfiguration for DHCPv4 is available through a partial implementation of RFC 3203, DHCP Reconfigure Extension for DHCPv4. It enables the DHCPv4 local server to send a message to the client to force reconfiguration.

The server sends a forcerenew message to a DHCPv4 client, initiating a message exchange. In response, DHCPv4 clients that support the forcerenew message then send a lease renewal message to the server. The server rejects the lease renewal request and sends a NAK to the client, causing the client to reinitiate the DHCP connection. A successful reconnection results in the reconfiguration of the DHCP client. Only the exchange of forcerenew, renew, and NAK messages is supported from RFC 3202. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to forcerenew messages other than to forward them to the client.
When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber services or DHCP-managed services, such as forwarding and statistics, continue to work. Client statistics are not maintained in the interval between a successful reconfiguration and the subsequent client binding. When the server responds to the client renewal request with a NAK, the client entry is removed from the binding table and final statistics are reported. New statistics are collected when the client sends a discover message to establish a new session.

Dynamic Client/Server Interaction for DHCPv6

Dynamic reconfiguration for DHCPv6 is available through a partial implementation of RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6). It enables the DHCPv6 local server to send a message to the client to force reconfiguration.

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition to the renewing state and send a renew message to the server. The server returns a reply message with a lifetime of zero (0). The client transitions to the init state and sends a solicit message. The server sends an advertise message to indicate that it is available for service. The client sends a request for configuration parameters, which the server then includes in its reply. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to reconfigure messages other than to forward them to the client.

When a DHCPv6 server is triggered to initiate reconfiguration on a bound DHCPv6 client, the client transitions to the reconfigure state. All subscriber services, such as forwarding and statistics, continue to work. The server then sends the reconfigure message to the client. If the DHCPv6 client is already in the reconfigure state, the DHCPv6 server ignores the reconfiguration trigger. For clients in any state other than bound or reconfigure, the server clears the binding state of the client, as if the cleardhcpv6 server binding command had been issued.

Manually Forcing the Local Server to Initiate the Reconfiguration Process

You can force the local server to initiate the reconfiguration process for clients by issuing the request dhcp server reconfigure command for DHCPv4 clients, and the request dhcpv6 server reconfigure command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Action Taken for Events That Occur During a Reconfiguration

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. Table 55 on page 844 lists the actions taken in response to several different events.
### Table 55: Action Taken for Events That Occur During a Reconfiguration

<table>
<thead>
<tr>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.</td>
<td>Server drops packet and deletes client.</td>
</tr>
<tr>
<td>Server receives a request, renew, rebind, or init-reboot message from the client.</td>
<td>DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).</td>
</tr>
<tr>
<td>Server receives a release or decline message from the client.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The client lease times out.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The <strong>clear dhcp server binding</strong> command is issued.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The <strong>request dhcp server reconfigure (DHCPv4) or request dhcpv6 server reconfigure (DHCPv6)</strong> command is issued.</td>
<td>Command is ignored.</td>
</tr>
<tr>
<td>GRES or DHCP restart occurs.</td>
<td>Reconfiguration process is halted.</td>
</tr>
</tbody>
</table>

**Benefits of Dynamic Reconfiguration of DHCP Local Server Clients**

- Enable the DHCP local server to dynamically reconfigure DHCP clients, avoiding extended outages because of server configuration changes that otherwise require the server to wait for the client to renew its lease or rebind to the server.

**Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview**

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements. You can provide the statements at the `[edit system services dhcp-local-server reconfigure]` hierarchy level for
all DHCPv4 clients, and at the [edit system services dhcp-local-server dhcpv6 reconfigure] hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the [edit system services dhcp-local-server group group-name reconfigure] hierarchy level for DHCPv4 clients, and at the [edit system services dhcp-local-server dhcpv6 group group-name reconfigure] hierarchy level for DHCPv6 clients.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

   For DHCPv4:

   ```
   [edit system services dhcp-local-server]
   user@host# set reconfigure
   ```

   For DHCPv6:

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set reconfigure
   ```

2. (Optional) Enable dynamic reconfiguration for only the clients serviced by a group of interfaces.

   For DHCPv4:

   ```
   [edit system services dhcp-local-server group group-name]
   user@host# set reconfigure
   ```

   For DHCPv6:

   ```
   [edit system services dhcp-local-server dhcpv6 group group-name]
   user@host# set reconfigure
   ```

3. (Optional) Configure how the server attempts reconfiguration.

   See "Configuring Dynamic Reconfiguration Attempts for DHCP Clients" on page 847.

4. (Optional) Configure the response to a failed reconfiguration.

   See "Configuring Deletion of the Client When Dynamic Reconfiguration Fails" on page 848.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

   See "Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect" on page 848.
6. (Optional) Configure a token for rudimentary server authentication.
   See "Configuring a Token for DHCP Local Server Authentication" on page 782.

7. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.
   See "Preventing Binding of Clients That Do Not Support Reconfigure Messages" on page 789.

### Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the `all` option.

  ```bash
  user@host> request dhcp server reconfigure all
  ```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCPv4 client.

  ```bash
  user@host> request dhcp server reconfigure 192.168.27.3
  ```

- Specify the MAC address of a DHCPv4 client.

  ```bash
  user@host> request dhcp server reconfigure 00:00:5E:00:53:67
  ```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

  ```bash
  user@host> request dhcp server reconfigure interface fe-0/0/0.100
  ```

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

  ```bash
  user@host> request dhcp server reconfigure all logical-system ls-bldg5
  ```

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

  ```bash
  user@host> request dhcp server reconfigure all routing-instance ri-boston
  ```
Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending forcerenew or reconfigure messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.
   
   For DHCPv4:
   
   ```
   [edit system services dhcp-local-server reconfigure]
   user@host# set attempts 5
   ```
   
   For DHCPv6:
   
   ```
   [edit system services dhcp-local-server dhcpv6 reconfigure]
   user@host# set attempts 5
   ```

2. Specify the interval between reconfiguration attempts.

   For DHCPv4:
   
   ```
   [edit system services dhcp-local-server reconfigure]
   user@host# set timeout 8
   ```

   For DHCPv6:
   
   ```
   [edit system services dhcp-local-server dhcpv6 reconfigure]
   user@host# set timeout 8
   ```

To override the global configuration for a particular group of clients, include the statements at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.
Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-abort
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-abort
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure trigger]
user@host# set radius-disconnect
```
For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure trigger]
user@host# set radius-disconnect
```

To override the global configuration for a particular group of clients, include the statement at the [edit system services dhcp-local-server group group-name reconfigure trigger] hierarchy level or the [edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger] hierarchy level.

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1</td>
<td>Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements.</td>
</tr>
</tbody>
</table>

#### RELATED DOCUMENTATION

- DHCP for Switches | 751

### Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers

#### IN THIS SECTION

- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups | 850

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group. For this, you must configure a group of DHCP server addresses, and apply them as an active server group. For more information, read this topic.
Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group, by specifying that group with the `active-server-group` statement globally or at the group level (configured with the `group` statement). When you apply the active server group at the group level, it overrides a global active server group configuration. An active server group is sometimes referred to as a trusted group of servers.

For example, you might want to direct certain DHCP clients to a different DHCP server than other clients, and you have different relay configurations for the clients. You can configure an interface group for each set of clients, specifying the DHCP relay interfaces for the group and any other relay configuration. In each of these groups, you specify an active server group to which each client groups traffic is forwarded.

To configure a group of DHCP server addresses and apply them as an active server group:

1. Specify the name of the server group.
   - For DHCPv4 servers:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# set server-group server-group-name
     ```
   - For DHCPv6 servers:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# set server-group server-group-name
     ```

2. Add the IP addresses of the DHCP servers belonging to the group.
   ```
   [edit forwarding-options dhcp-relay server-group server-group-name]
   user@host# set ip-address1
   user@host# set ip-address2
   ```

   **NOTE:** Starting in Junos OS Release 18.4R1, up to 32 server IP addresses are supported per DHCPv4 server group. In earlier releases, a maximum of 5 server IP addresses are supported for DHCPv4 servers. Configuring more than the maximum number of server addresses results in a commit check failure.

3. Apply the server group as an active server group.
• For all DHCP clients, unless overridden:

```text
[edit forwarding-options dhcp-relay]
user@host# set active-server-group server-group-name
```

• For a group of DHCP relay interfaces, overriding the global active server group:

```text
[edit forwarding-options dhcp-relay group interface-group-name]
user@host# set active-server-group server-group-name
```

• For all DHCPv6 clients, unless overridden for a group:

```text
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set active-server-group server-group-name
```

• For a group of DHCPv6 relay interfaces, overriding the global active server group:

```text
[edit forwarding-options dhcp-relay dhcpv6 group interface-group-name]
user@host# set active-server-group server-group-name
```

Consider the following example. Three groups of DHCP server addresses are configured, Default, Campus-A, and Campus-B. The Default group is applied as the global active server group for the overall DHCP relay configuration.

The Campus-A server group is assigned as the active server group for interface group Campus-A-v10-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-A-v10-DHCP-RELAY is forwarded to DHCP servers 198.51.100.100 and 198.51.100.101.

The Campus-B server group is assigned as the active server group for interface group Campus-B-v200-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-B-v200-DHCP-RELAY is forwarded to DHCP servers 198.51.100.55 and 198.51.100.56.

All other DHCP traffic is forwarded to DHCP server 203.0.113.1.

```text
[edit forwarding-options dhcp-relay]
#
# Server groups
user@host# set server-group Default 203.0.113.1
user@host# set server-group Campus-A 198.51.100.100
user@host# set server-group Campus-A 198.51.100.101
user@host# set server-group Campus-B 198.51.100.55
user@host# set server-group Campus-B 198.51.100.56
#
```
In some configurations, servers in an active server group maintain redundant information about the DHCP clients. If the binding server later becomes inaccessible, the client is unable to renew the lease from that server. When the client attempts to rebind to a server, other servers in the group with the client information can reply with an ACK message. By default, instead of forwarding the ACK to the DHCP client, the relay agent drops any such ACKs that it receives from any server other than the binding server because the new server address does not match the expected server address in the DHCP client entry. Consequently the lease cannot be extended by any of the redundant servers.

Starting in Junos OS Release 16.2R1, you can enable a DHCPv4 relay agent to forward DHCP request (renew or rebind) ACKs from any server in the active server group (thus, any trusted server). The relay agent updates the client entry with the new server address. Because the servers in the group are expected to mirror the client information exactly, the lease option is expected to be the same as for the original server and the relay agent does not need to verify the lease option.

Starting in Junos OS Release 18.4R1, this capability is extended to allow a DHCP relay agent to forward DHCP information request (DHCPINFORM) ACK messages from any server in the active server group.

To enable ACK forwarding from any server in the active server group:

- Enable forwarding for the active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set allow-server-change
```

### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.4R1</td>
<td>Starting in Junos OS Release 18.4R1</td>
</tr>
<tr>
<td>16.2R1</td>
<td>Starting in Junos OS Release 16.2R1</td>
</tr>
</tbody>
</table>
Grouping Interfaces and Applying a Common DHCP Configuration to the Group

In this Section

- Grouping Interfaces with Common DHCP Configurations | 853
- Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces | 854
- Configuring Group-Specific DHCP Local Server Options | 856
- Configuring Group-Specific DHCP Relay Options | 856

You use the group feature to group a set of interfaces and then apply a common DHCP configuration such as extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent to the named interface group. For more information, read this topic.

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

    [edit system services]
    user@host# edit dhcp-local-server
2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface interface-name` statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the `upto` option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

### Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```
- The start subunit, `interface interface-name`, serves as the key for the stanza. The remaining configuration settings are considered attributes.

- If the subunit is not included, an implicit .0 subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, `interface ge-2/2/2` is treated as `interface ge-2/2/2.0`.

- Ranged entries contain the `upto` option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a 0 (zero) subunit acts as a wildcard.

- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.

- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because `ge-1/0/0.10` is the start subunit for both.

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.10
  ```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface `ge-1/0/0.26` is common to all three.

  ```
  dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
  ```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.20 upto ge-1/0/0.40
  ```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

  In the following example, the three ranges nest properly:

  ```
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
  interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
  ```
Discrete interfaces take precedence over ranges. In the following example, interface `ge-1/0/0.20` takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

### Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the `[edit system services dhcp-local-server group group-name]` hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the `[edit system services dhcp-local-server group group-name]` hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the `[edit system services dhcp-local-server]` hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the `dynamic-profile` statement.

- **authentication**—Configure the parameters the router sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **liveness-detection**—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see "DHCP Liveness Detection Overview" on page 858.
- **overrides**—Override the default configuration settings for the extended DHCP local server. For information, see "Overriding the Default DHCP Local Server Configuration Settings Overview" on page 807.

### Configuring Group-Specific DHCP Relay Options

You can include the following statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level to configure group-specific options for DHCPv6 relay agent.
• **active-server-group**—Configure an active server group to apply a common DHCP relay agent configuration for a named group of DHCP server addresses. For information, see "Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups" on page 850.

• **authentication**—Configure the parameters the router (or switch) sends to the external AAA server.

• **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.

• **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.

• **liveness-detection**—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see "DHCP Liveness Detection Overview" on page 858.

• **overrides**—Override the default configuration settings for the extended DHCP relay agent. For information, see "Overriding the Default DHCP Relay Configuration Settings" on page 803.

• **relay-agent-interface-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

• **relay-agent-remote-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.

• **relay-option**—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see *Using DHCP Option Information to Selectively Process DHCP Client Traffic*.

• **relay-option-82**—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see “Using DHCP Relay Agent Option 82 Information” on page 739.

• **service-profile**—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see *Default Subscriber Service Overview*.

**RELATED DOCUMENTATION**

| Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers | 849 |
| DHCP for Switches | 751 |
Connectivity Liveness Detection in the DHCP Access Network

IN THIS SECTION

- DHCP Liveness Detection Overview | 858
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD | 860
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
- Configuring Detection of DHCP Local Server Client Connectivity with BFD | 866
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 873

DHCP Liveness Detection Overview

Unlike PPP, DHCP does not define a native keepalive mechanism as part of either the DHCPv4 or DHCPv6 protocols. Without a keepalive mechanism, DHCP local server, DHCP relay, and DHCP relay proxy are unable to quickly detect if any of them has lost connectivity with a subscriber or a DHCP client. Instead, they must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages before exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often insufficient when serving as session health checks for clients in a DHCP subscriber access or a DHCP-managed network. Because DHCP lease times are typically too long to provide an adequate response time for a session health failure, and configuring short DHCP lease times can pose an undue burden on control plane processing, implementing a DHCP liveness detection mechanism enables better monitoring of bound DHCP clients. When configured with a liveness detection protocol, if a given subscriber (or client) fails to respond to a configured number of consecutive liveness detection requests, the subscriber (or client) binding is deleted and its resources released.

DHCP liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.
Using DHCP liveness detection, IP sessions are acted upon as soon as liveness detection checks fail. This faster response time serves to:

- Provide more accurate time-based accounting of subscriber (or DHCP client) sessions.
- Better preserve router (switch) resources.
- Help to reduce the window of vulnerability to some security attacks.

Examples of liveness detection protocols include Bidirectional Forwarding Detection (BFD) for both DHCPv4 and DHCPv6 subscribers, IPv4 Address Resolution Protocol (ARP) for DHCPv4 subscribers, and IPv6 Neighbor Unreachability Detection (NUD) using Neighbor Discovery (ND) packets for DHCPv6 subscribers.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. In earlier releases, only BFD is supported for all platforms.

The two liveness detection methods are mutually exclusive.

When configuring BFD liveness detection, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 liveness detection either globally or per DHCPv4 or DHCPv6 group.
- DHCPv4 or DHCPv6 subscriber access clients that do not support BFD are not affected by the liveness detection configuration. These clients can continue to access the network (after they are validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for clients that support BFD when those clients enter a bound state.
- After protocol-specific messages are initiated for a BFD client, they are periodically sent to the subscriber (or client) IP address of the client and responses to those liveness detection requests are expected within a configured amount of time.
- If liveness detection responses are not received from clients that support BFD within the configured amount of time for a configured number of consecutive attempts, the liveness detection check is deemed to have failed. A configured failure action to clear the client binding is applied.
- The only failure action supported for Layer 2 Liveness detection is clear-binding.

When configuring DHCP ARP and ND Layer 2 liveness detection on MX Series, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 ARP and ND liveness detection globally, per DHCPv4 or DHCPv6 group, and per dual-stack group.
- ARP/ND liveness detection applies only to DHCP clients that:
• Are directly connected over dynamic VLANs.
• Have permanent Layer 2 entries.
• DHCPv6 clients must have a unique source MAC address and link-local address. Only single liveness detection entry is used for all IPv6 addresses associated with a specific client session.

## Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP relay clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.
   
   - For DHCP global configuration:
     
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection
     ```
   
   - For DHCP group configuration:
     
     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit liveness-detection
     ```

   **NOTE:** Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.

   ```
   [edit forwarding-options dhcp-relay group group-name]
   user@host# set overrides proxy-mode
   ```
3. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:
  
  ```plaintext
  [edit forwarding-options dhcp-relay liveness-detection]
  user@host# edit method
  ```

- For DHCP group configuration:
  
  ```plaintext
  [edit forwarding-options dhcp-relay group group-name liveness-detection]
  user@host# edit method
  ```

4. Specify the liveness detection method that you want DHCP to use.

**NOTE:** In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:
  
  ```plaintext
  [edit forwarding-options dhcp-relay liveness-detection method]
  user@host# edit bfd
  ```

- For DHCP group configuration:
  
  ```plaintext
  [edit forwarding-options dhcp-relay group group-name liveness-detection method]
  user@host# edit bfd
  ```

5. Configure the liveness detection method as desired.

See “Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients” on page 862 for an example of how to globally configure DHCP relay liveness detection with BFD.

6. Configure the action the router takes when a liveness detection failure occurs.

- For DHCP global configuration:
  
  ```plaintext
  [edit forwarding-options dhcp-relay liveness-detection]
  ```
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

IN THIS SECTION

- Requirements | 862
- Overview | 863
- Configuration | 863

This example shows how to configure liveness detection for DHCP relay agent subscribers using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers.
- Junos OS Release 12.1 or later

Before you begin:
Configure DHCP relay agent. See "Extended DHCP Relay Agent Overview" on page 792.

Overview

In this example, you configure liveness detection for DHCP relay agent subscribers by completing the following operations:

1. Enable liveness detection globally for DHCP relay subscribers.

2. Specify BFD as the liveness detection method for all dynamically created DHCP relay subscribers.

3. Configure BFD-specific statements to define how the protocol behaves.

4. Configure the action the router takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the [edit forwarding-options dhcp-relay dhcpv6] or [edit forwarding-options dhcp-relay dhcpv6 group group-name] hierarchy level.

Configuration

Step-by-Step Procedure

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.

   [edit forwarding-options dhcp-relay]
   user@host# edit liveness-detection

2. Specify that you want to configure the liveness detection method.

   [edit forwarding-options dhcp-relay liveness-detection]
   user@host# edit method

3. Specify BFD as the liveness detection method that you want DHCP to use.
4. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set detection-time threshold 50000
```

5. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set holddown-interval 50
```

6. Configure the BFD minimum transmit and receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-interval 45000
```

7. Configure the minimum receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

8. Configure a multiplier value for the detection time.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set multiplier 100
```

9. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set no-adaptation
```

10. Configure the BFD session mode.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
```
11. Configure the threshold and minimum interval for the BFD transmit interval.

```plaintext
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

12. Configure the BFD protocol version you want to detect.

```plaintext
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set version automatic
```

13. Configure the action the router takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```plaintext
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

**Results**

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```plaintext
[edit]
user@host# show forwarding-options
dhcp-relay {
  liveness-detection {
    failure-action clear-binding-if-interface-up;
    method {
      bfd {
        version automatic;
        minimum-interval 45000;
        minimum-receive-interval 60000;
        multiplier 100;
        no-adaptation;
        transmit-interval {
          minimum-interval 45000;
          threshold 60000;
        }
      }
    }
  }
}
```
If you are done configuring the device, enter `commit` from configuration mode.

### Configuring Detection of DHCP Local Server Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP local server clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

**NOTE:** You can also configure DHCP liveness detection for DHCP relay.
To configure liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:
     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection
     ```
   - For DHCP group configuration:
     ```
     [edit system services dhcp-local-server group group-name]
     user@host# edit liveness-detection
     ```

   **NOTE:** Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

2. Specify that you want to configure the liveness detection method.
   - For DHCP global configuration:
     ```
     [edit system services dhcp-local-server liveness-detection]
     user@host# edit method
     ```
   - For DHCP group configuration:
     ```
     [edit system services dhcp-local-server group group-name liveness-detection]
     user@host# edit method
     ```

3. Specify the liveness detection method that you want DHCP to use.
NOTE: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

4. Configure the liveness detection method as desired.

   See "Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients" on page 869 for an example of how to configure DHCPv4 groups for DHCP local server liveness detection with BFD.

5. Configure the action the router takes when a liveness detection failure occurs.

   - For DHCP global configuration:

     [edit system services dhcp-local-server liveness-detection]
     user@host# edit failure-action action

   - For DHCP group configuration:

     [edit system services dhcp-local-server group group-name liveness-detection]
     user@host# edit failure-action action
Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

This example shows how to configure group liveness detection for DHCP local server subscribers or DHCP clients using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP local server. See “Extended DHCP Local Server Overview” on page 718.

Overview

In this example, you configure group liveness detection for DHCP local server subscribers (clients) by completing the following operations:

1. Enable liveness detection for DHCP local server subscriber (or DHCP client) groups.

2. Specify BFD as the liveness detection method for all dynamically created DHCP local server subscribers (clients).

3. Configure BFD-specific statements to define how the protocol behaves.

4. Configure the action the router (switch) takes when a liveness detection failure occurs.
NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

**Configuration**

**Step-by-Step Procedure**

To configure group liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.
   ```
   [edit system services dhcp-local-server ]
   user@host# edit liveness-detection
   ```

2. Specify that you want to configure liveness detection for a specific DHCP local server group.
   ```
   [edit system services dhcp-local-server liveness-detection]
   user@host# edit group local_group_1
   ```

3. Specify that you want to configure the liveness detection method.
   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection]
   user@host# edit method
   ```

4. Specify BFD as the liveness detection method that you want DHCP to use.
   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method]
   user@host# edit bfd
   ```

5. Configure the detection time threshold (in milliseconds) at which a trap is produced.
   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set detection-time threshold 30000
   ```
6. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set holddown-interval 50
```

7. Configure the BFD minimum transmit and receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum transmit and receive interval if you configure the minimum-interval for the BFD transmit-interval statement and the minimum-receive-interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set minimum-interval 45000
```

8. Configure the minimum receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum receive interval if you configure the BFD minimum transmit and receive interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

9. Configure a multiplier value for the detection time.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set multiplier 100
```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set no-adaptation
```

11. Configure the BFD session mode.
12. Configure the threshold and minimum interval for the BFD transmit interval.

![NOTE: You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.]

13. Configure the BFD protocol version you want to detect.

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

Results
From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.
version automatic;
minimum-interval 45000;
minimum-receive-interval 60000;
multiplier 100;
no-adaptation;
transmit-interval {
    minimum-interval 45000;
    threshold 60000;
}
detection-time {
    threshold 30000;
}
session-mode automatic;
holddown-interval 50;
}
}
}
}
}

If you are done configuring the device, enter commit from configuration mode.

### DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

#### IN THIS SECTION
- How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works | 873
- Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets | 877
- Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets | 879
- Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets | 882

### How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works

Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients. This Layer 2 liveness detection offers separate mechanisms for the DHCP client host and for the router acting
as a broadband network gateway (BNG) to determine the validity and state of the DHCP client sessions. These mechanisms are referred to as the send functionality and the receive functionality. You can configure Layer 2 liveness detection for DHCP local server and DHCP relay clients.

Send Functionality

The BNG uses the send functionality to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions. Figure 41 on page 874 illustrates the send functionality.

Figure 41: Layer 2 Liveness Detection Send Behavior Flow
1. The BNG sends request packets to the each DHCP client at a configurable interval, then waits for a response. The BNG retries the requests when it does not receive a timely response. It sends ARP requests for DHCPv4 clients and Neighbor Discovery (ND) requests for DHCPv6 clients.

2. If the BNG receives a response from the client before the interval times out, it waits for the timer to expire and then sends another request to that client.

3. If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt; the timer is not configurable.

4. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

5. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This timer value is not configurable.

6. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

7. If the BNG does not receive a response within the 10-second interval, it sends another request and starts the 10-second timer again. The BNG continues to send requests at 10-second intervals until it receives a response from the client before the interval times out or it exhausts the number of retry attempts.

   The first retry attempt uses the 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

8. If the BNG never sends a response from a client within the interval before the retries are exhausted, then the liveness detection check fails and the clear-binding failure action is implemented. The client session is cleared.

**Receive Functionality**

The receive functionality enables a DHCP client host to determine the state of the DHCPv4 or DHCPv6 client session from the perspective of a BNG. The BNG conducts a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients when it receives ARP or ND packets. Figure 42 on page 876 illustrates the receive functionality.
When the BNG receives either of these packets, it does the following:

1. Checks whether Layer 2 liveness detection for subscriber management is enabled globally for the relevant address family, inet or inet6.

2. If Layer 2 liveness detection is not enabled, then the BNG responds as usual to the received packets without checking the state of the client session.

3. If liveness detection is enabled for the family, then the BNG checks whether the client session is still in the bound state.

4. If the client session is bound, the BNG responds to the client with the appropriate ARP or ND packet.

5. If the session is not bound, the BNG drops the received packet. It does not send an ARP or ND response packet to the host, enabling the host to determine that the BNG considers the session to be down.

The usefulness of the receive functionality depends on the ability of the DHCP client host to reclaim resources from the stale client based on the absence of a response packet from the BNG for an unbound client session. If this capability requires a change in the client implementation, you may want to use the send functionality.
Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 local server liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:
     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection method
     ```
   - For DHCPv4 group configuration:
     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name liveness-detection method
     ```
   - For DHCPv4 dual-stack-group configuration:
     ```
     [edit system services dhcp-local-server]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:
     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# set layer2-liveness-detection
     ```
   - For DHCPv4 group configuration:
     ```
     [edit system services dhcp-local-server group group-name liveness-detection method]
     user@host# set layer2-liveness-detection
     ```
• For DHCPv4 dual-stack-group configuration:

```bash
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

• For DHCPv4 global configuration:

```bash
[edit system services dhcp-local-server liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

• For DHCPv4 group configuration:

```bash
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

• For DHCPv4 dual-stack-group configuration:

```bash
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 local server liveness detection:

1. Specify that you want to configure the liveness detection method.

• For DHCPv6 global configuration:

```bash
[edit system services dhcp-local-server dhcpv6]
user@host# edit liveness-detection method
```

• For DHCPv6 group configuration:

```bash
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

• For DHCPv6 global configuration:
Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP relay clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 relay liveness detection:

1. Specify that you want to configure the liveness detection method.

   • For DHCPv4 global configuration:
• For DHCPv4 group configuration:

[edit forwarding-options dhcp-relay]
user@host# edit group {group-name} liveness-detection method

• For DHCPv4 dual-stack-group configuration:

[edit forwarding-options dhcp-relay]
user@host# edit dual-stack-group {dual-stack-group-name} liveness-detection method

2. Specify the Layer 2 liveness detection method.

• For DHCPv4 global configuration:

[edit forwarding-options dhcp-relay liveness-detection method]
user@host# set layer2-liveness-detection

• For DHCPv4 group configuration:

[edit forwarding-options dhcp-relay group {group-name} liveness-detection method]
user@host# set layer2-liveness-detection

• For DHCPv4 dual-stack-group configuration:

[edit forwarding-options dhcp-relay dual-stack-group {dual-stack-group-name} liveness-detection method]
user@host# set layer2-liveness-detection

3. (Optional) Configure the number of retry attempts and the interval timer.

• For DHCPv4 global configuration:

[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds

• For DHCPv4 group configuration:

[edit forwarding-options dhcp-relay group {group-name} liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds

- For DHCPv4 dual-stack-group configuration:

  [edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection method]
  user@host# edit layer2-liveness-detection
  user@host# set max-consecutive-retries number
  user@host# set transmit-interval seconds

To configure the send functionality for DHCPv6 relay liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv6 global configuration:

     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit liveness-detection method

   - For DHCPv6 group configuration:

     [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
     user@host# edit group group-name liveness-detection method

2. Specify the Layer 2 liveness detection method.
   - For DHCPv6 global configuration:

     [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
     user@host# set layer2-liveness-detection

   - For DHCPv6 group configuration:

     [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
     user@host# set layer2-liveness-detection

3. (Optional) Configure the number of retry attempts and the interval timer.
   - For DHCPv6 global configuration:

     [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
     user@host# edit layer2-liveness-detection
     user@host# set max-consecutive-retries number
     user@host# set transmit-interval seconds
For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the receive functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The receive functionality enables the DHCP client host to determine whether a client session is down based on a lack of response from the BNG to the ARP or ND packets it sends to the BNG. You configure the receive functionality globally for DHCP per address family as an override to the global subscriber management configuration.

1. Enable Layer 2 liveness detection globally per address family.

   - For DHCPv4:

     ```
     [edit system services subscriber-management overrides]
     user@host# set interfaces family inet layer2-liveness-detection
     ```

   - For DHCPv6:

     ```
     [edit system services subscriber-management overrides]
     user@host# set interfaces family inet6 layer2-liveness-detection
     ```

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4R1</td>
<td>Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.</td>
</tr>
</tbody>
</table>
Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.

Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

### RELATED DOCUMENTATION

- **DHCP Overview**

### Securing DHCP Messages Sent Between DHCP Clients and Servers in Different VRFs

Junos OS allows you to use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs. To exchange DHCP messages between different VRFs, you must enable
both the server side and the client side of the DHCP relay agent recognize and forward acceptable traffic based on DHCP option information in the packets. The DHCP relay agent can ensure that there is no direct routing between the client virtual routing and forwarding instance (VRF) and the DHCP server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. For more information, read this topic.

### DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs

In some service provider networks, the service network in which the DHCP server resides is isolated from the actual subscriber network. This separation of the service and subscriber networks can sometimes introduce potential security issues, such as route leaking. Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs. The DHCP relay agent can ensure that there is no direct routing between the client virtual routing and forwarding instance (VRF) and the DHCP server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. Subscriber management supports the cross-VRF message exchange for both DHCP and DHCPv6 packets.

To exchange DHCP messages between different VRFs, you must enable both the server side and the client side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information in the packets. The message exchange uses the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets and the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets to identify traffic to be relayed.

Statistics for DHCP packets using the cross-VRF message exchange are counted in the client VRF.

The following list describe how DHCP relay agent exchanges messages between the DHCP clients and DHCP server in different VRFs:

- **Packets from DHCP client to DHCP server**—DHCP relay agent receives the DHCP packet from the client in the client VRF, and then inserts the appropriate DHCP option 82 suboption 1 or DHCPv6 option 18 attribute into the packet. The relay agent then forwards the packet to the DHCP server in the server's VRF.

- **Packets from DHCP server to DHCP client**—DHCP relay agent receives the DHCP reply message from the DHCP server in the server VRF. The relay agent derives the client's interface, including VRF, from the DHCP option 82 suboption 1 or DHCPv6 option 18 attribute in the packet in the DHCP server VRF. The relay agent then forwards the reply message to the DHCP client in the client's VRF.
Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances

Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for a stateless DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that must be isolated from the client network.

A stateless DHCP relay agent does not maintain dynamic state information about the DHCP clients and does not maintain a static route for the traffic to flow between the client and server routing instances.

To enable the DHCP message exchange between the two VRFs, you configure each side of the DHCP relay to recognize and forward acceptable traffic based on the DHCP option information in the packets. The acceptable traffic is identified by either the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets or the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets.

The following list provides an overview of the tasks required to create the DHCP message exchange between the different VRFs:

- **Client-side support**—Configure the DHCP relay agent `forward-only` statement to specify the VRF location of the DHCP server, to which the DHCP relay agent forwards the client packets with the appropriate DHCP option information. The `forward-only` statement ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations (such as creating dynamic interfaces or maintaining leases).

  You can optionally configure a specific logical system and routing instance for the server VRF. If you do not specify a logical system or routing instance, then DHCP uses the local logical system and routing instance from which the configuration is added.

- **Server-side support**—Configure the DHCP relay agent `forward-only-replies` statement so the DHCP relay agent forwards the reply packets that have the appropriate DHCP option information. This statement
also ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations.

**NOTE:** You do not need to configure the `forward-only-replies` statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

- **DHCP local server support**—Configure the DHCP local server to support option 82 information in DHCP NAK and forcerenew messages. By default, the two message types do not support option 82.

- **Additional support**—Ensure that the following required support is configured:
  - Proxy ARP support must be enabled on the server-facing interface in the DHCP server VRF so that the DHCP relay agent can receive and respond to the ARP requests for clients and the client-facing interface in the DHCP server VRF.
  - Routes must be available to receive the DHCP packets from the DHCP server in the server VRF for the clients reachable in the client VRF.

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different VRFs.

### Client-Side Support

To configure support on the client side of the DHCP relay agent:

1. Enable DHCP relay agent configuration.

   ```
   [edit forwarding-options]
   user@host# edit dhcp-relay
   ```

2. Specify the DHCP server VRF to which the DHCP relay agent forwards the packets from the DHCP client. DHCP relay agent forwards the acceptable packets that have the appropriate DHCP option information, but does not perform any additional subscriber management operations. You can configure the `forward-only` statement globally or for a named group of interfaces, and for DHCPv4 or DHCPv6. You can specify the current, default, or a specific logical system or routing instance for the server VRF.

   The following example configures the `forward-only` statement globally for DHCPv4, and specifies the default logical system and routing instance:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# set forward-only logical-system default routing-instance default
   ```
NOTE: For local DHCPv4 clients, the DHCP relay agent adds the Agent Circuit ID option. However, if the Agent Circuit ID option is already present in the packet, you must ensure that the DHCP server supports the option 82 Vendor-Specific Information suboption (suboption 9).

If the forward-only statement is configured at the [edit forwarding-options dhcp-relay relay-option] hierarchy level, then that relay-option action takes precedence over the configuration of the forward-only statement for the DHCP cross-VRF message exchange.

Server-Side Support

To configure the cross-VRF message exchange support on the server side of the DHCP relay:

NOTE: You do not need to configure the forward-only-replies statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

1. Enable DHCP relay agent configuration.

   [edit forwarding-options]
   user@host# edit dhcp-relay

2. Configure the DHCP relay agent to forward the DHCP packets from the DHCP server VRF to the client. DHCP relay agent only forwards the packets, and does not perform any additional subscriber management operations. You can configure the forward-only-replies statement globally for DHCPv4 and DHCPv6.

   The following example configures the forward-only-replies statement globally for DHCPv4.

   [edit forwarding-options dhcp-relay]
   user@host# set forward-only-replies

DHCP Local Server Support

To configure the DHCP local server to support option 82 information in NAK and forcerenew messages; the cross-VRF message exchange feature uses the option 82 or DHCPv6 option 18 information to determine the client VRF:

1. Enable DHCP local server configuration.
2. Specify that you want to configure an override option.

```
[edit system services]
user@host# edit dhcp-local-server
```

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

3. Configure DHCP local server to override the default behavior and support option 82 information in DHCP NAK and forcerenew messages. You can configure the override action globally, for a group of interfaces, or for a specific interface.

```
[edit system services dhcp-local-server overrides]
user@host# set include-option-82 forcerenew nak
```

**Release History Table**

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different VRFs.</td>
</tr>
<tr>
<td>14.2</td>
<td>Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).</td>
</tr>
</tbody>
</table>

**RELATED DOCUMENTATION**

- DHCP for Switches | 751
Assigning IP Addresses for DHCP

IN THIS SECTION

- Address-Assignment Pools Overview | 889
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 891
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching | 893
- Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option | 893
- Multiple Address Assignment for DHCPv6 Clients | 894

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You can create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. For more information, read this topic.

Address-Assignment Pools Overview

The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. The authd process manages the pools and the address allocation, whether the addresses come from local pools or from a RADIUS server. For example, multiple client applications, such as DHCP, can use the same address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients. The pool selected for a subscriber, based on the RADIUS server or network matching or other rule, is called the matching pool for the subscriber.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, which is supported for IPv4 pools only, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

You can configure named address ranges within an address-assignment pool. A named range is a subset of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, for IPv4 address-assignment pools, you might create a named
range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.

Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool. For example, you might want to reserve certain addresses or ranges to be used only for static subscribers. When you configure an address or range to be excluded, and the address or an address within the range, has already been allocated, that subscriber is logged out, the address is deallocated, and the address is marked for exclusion.

You can link address-assignment pools together to provide backup pools for address assignment. When no addresses are found to be available in the primary or matching address pool, the router or switch automatically proceeds to the linked (secondary) address pool to search for an available address to allocate.

Although the first pool in a chain of linked pools is generally considered the primary pool, a matching pool is not necessarily the first pool in the chain. For example, in a chain of three pools, A, B, and C, where A is the primary pool, pool B might be matched for certain subscribers based on information returned by the RADIUS server. The search for an available address for those subscribers begins in pool B.

Starting in Junos OS Release 18.1R1, the behavior changes for how the search for an available address proceeds through a chain of linked pools. By default, the matching pool is searched first, then the search moves to the first pool in the chain and proceeds through the chain until an available address is found and allocated, or until the search determines no addresses are free. In each pool, all address ranges are fully searched for an address. This behavior enables addresses to be assigned contiguously.

Alternatively, you can configure the `linked-pool-aggregation` statement to search first within a block of addresses in each range in the matching pool and then successively through the linked pools. The search then moves back to the first pool in the chain and searches all addresses in all ranges in each pool through the last pool in the chain.

The address-assignment pool hold-down feature enables you to specify that no additional address are allocated from an existing active address-assignment pool. This configuration gracefully transforms the active pool to an inactive state as the previously allocated addresses are returned to the pool. When the pool is inactive, you can safely perform maintenance on the pool without affecting any active subscribers.

You can also explicitly identify that an address-assignment pool is used for NDRA.

**NOTE:** This feature requires a license. To understand more about Subscriber Access Licensing, see [Subscriber Access Licensing Overview](#). Please refer to the [Juniper Licensing Guide](#) for general information about License Management. Please refer to the product [Data Sheets](#) for details, or contact your Juniper Account Team or Juniper Partner.
Benefits of Address Assignment Pools

- You can create centralized pools of addresses independent of client applications.
- You can specify blocks of addresses, named ranges, so that a given address pool can be used to supply different addresses for different client applications or for subscribers that match different sets of criteria.
- You can link pools together to ensure that pools are searched for free addresses in a specific manner, contiguously or noncontiguously.
- You can gracefully transition an address pool from active to inactive by specifying that no further addresses are allocated from the pool.

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

You can specify the match order in which the extended DHCP local server uses the client data to determine the address-assignment pool that provides the IP address and configuration for a DHCP client. You use the `pool-match-order` statement to specify the match order. If you do not specify the `pool-match-order`, the router (or switch) uses the default `ip-address-first` matching to select the address pool. After DHCP local server determines the address assignment pool to use, the server performs the matching based on the criteria you specified in the pool configuration.

In the default `ip-address-first` matching, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address. If there is no giaddr in the request, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

In `external-authority` matching, the DHCP local server receives the address assignment from an external authority, such as RADIUS or Diameter. If RADIUS is the external authority, the DHCP local server uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. If Diameter is the external authority, the server uses the Diameter counterpart of the Framed-IPv6-Pool attribute to determine the pool.

For IPv4 address-assignment pools, you can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.
NOTE: To use the DHCP local server option 82 matching feature with an IPv4 address-assignment pool, you must ensure that the `option-82` statement is included in the `dhcp-attributes` statement for the address-assignment pool.

To configure the matching order the extended DHCP local server uses to determine the address-assignment pool used for a client:

1. Access the `pool-match-order` configuration.

   ```
   [edit system services dhcp-local-server]
   user@host# edit pool-match-order
   ```

2. Specify the pool matching methods in the order in which the router (switch) performs the methods. You can specify the methods in any order. All methods are optional—the router (switch) uses the `ip-address-first` method by default.
   
   - Configure the router (switch) to use an external addressing authority.
   ```
   [edit system services dhcp-local-server pool-match-order]
   user@host# set external-authority
   ```

   - Configure the router (switch) to use the `ip-address-first` method.
   ```
   [edit system services dhcp-local-server pool-match-order]
   user@host# set ip-address-first
   ```

   - (IPv4 address-assignment pools only) Specify the option 82 matching method.
   ```
   [edit system services dhcp-local-server pool-match-order]
   user@host# set option-82
   ```
Example: Extended DHCP Local Server Configuration with Optional Pool Matching

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
pool-match-order {
    external-authority
    ip-address-first;
    option-82;
}
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option

Subscriber management or DHCP management enables you to specify that DHCP local server assign a particular address to a client. For example, if a client is disconnected, you might use this capability to assign the same address that the client was using prior to being disconnected. If the requested address is available,
DHCP assigns it to the client. If the address is unavailable, the DHCP local server offers another address, based on the address allocation process.

Both DHCP local server and DHCPv6 local server support the specific address request feature. DHCP local server uses DHCP option 50 in DHCP discover messages to request a particular address, while DHCPv6 local server uses the IA_NA option (Identity Association for Non-Temporary Addresses) in DHCPv6 solicit messages.

NOTE: Subscriber management (DHCP management) supports only one address for each of the DHCPv6 IA_NA or IA_PD address types. If the DHCPv6 client requests more than one address for a given type, the DHCPv6 local server uses only the first address and ignores the other addresses.

### Multiple Address Assignment for DHCPv6 Clients

For a DHCPv6 local server, you can assign multiple addresses to a single DHCPv6 client. Multiple address support is enabled by default, and is activated when the DHCPv6 local server receives a DHCPv6 Solicit message from a DHCP client that contains multiple addresses.

For example, if you are implementing this feature on the routers, you might use the multiple address assignment feature when a customer premises equipment (CPE) device requires a host address and a delegated prefix.

You can use either local address pools or RADIUS when assigning multiple addresses to a DHCP client. When at least one address is successfully allocated, the switch creates a DHCP client entry and binds the entry to the assigned address. If both addresses are successfully allocated, the switch creates a single DHCP client entry and binds both addresses to that entry.

You can also configure a delegated address pool, which explicitly specifies the address pool that DHCP management uses to assign IPv6 prefixes for DHCP clients.

SEE ALSO

* Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*
### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.1R1</td>
<td>Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool.</td>
</tr>
<tr>
<td>18.1R1</td>
<td>Starting in Junos OS Release 18.1R1, the behavior changes for how the search for an available address proceeds through a chain of linked pools.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- **DHCP for Switches** | 751

### Suppressing DHCP Access

#### IN THIS SECTION

- Suppressing DHCP Access, Access-Internal, and Destination Routes | 896
- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | 897

The DHCP process adds access-internal and destination routes for DHCPv4 sessions, and access-internal and access routes for DHCPv6 sessions during the DHCP client binding operation. However, you can override the default behavior and prevent DHCP from automatically installing the route information. For more information, read this topic.
Suppressing DHCP Access, Access-Internal, and Destination Routes

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds access-internal and destination routes for DHCPv4 sessions, and access-internal and access routes for DHCPv6 sessions. In some scenarios, you might want to override the default behavior and prevent DHCP from automatically installing the route information. For example, DHCP relay installs destination (host) routes by default—this action is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of destination routes might cause a conflict when you configure DHCP relay with static subscriber interfaces. To avoid such configuration conflicts you can override the default behavior and prevent DHCP relay from installing the routes.

NOTE: You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.

You can configure both DHCP local server and DHCP relay agent to override the default route installation behavior, and you can specify the override for both DHCPv4 and DHCPv6 sessions. You can override the route installation globally or for named interface groups. For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both.
Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default

You can configure both DHCP local server and DHCP relay agent to override the default installation of access, access-internal, and destination routes. For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both. You can configure the override globally or for named interface groups.

**NOTE:** You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.

**NOTE:** The `no-arp` statement is deprecated and the function is replaced by the `route-suppression` statement.

To configure route suppression and prevent DHCP from installing specific types of routes:

- **For DHCP local server route suppression (for example, a global configuration):**

  ```
  [edit system services dhcp-local-server]
  user@host# set route-suppression access-internal
  ```

- **For DHCP relay (for example, a group-specific configuration):**

  ```
  [edit forwarding-options dhcp-relay group southeast]
  user@host# set route-suppression destination
  ```

- **For DHCPv6 local server (for example, a group-specific configuration):**

  ```
  [edit system services dhcp-local-server group southern3]
  user@host# set dhcpv6 route-suppression access access-internal
  ```

- **For DHCPv6 relay (for example, a global configuration):**

  ```
  [edit forwarding-options dhcp-relay]
  user@host# set dhcpv6 route-suppression access
  ```
DHCP Snooping

IN THIS SECTION

- DHCP Snooping Support | 898
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent | 900
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | 902

DHCP snooping on Junos OS device validates DHCP messages and drops invalid traffic. You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP Snooping Support

DHCP snooping provides DHCP security by identifying incoming DHCP packets. In the default DHCP snooping configuration, all traffic is snooped. You can optionally use the forward-snooped-clients statement to evaluate the snooped traffic and to determine if the traffic is forwarded or dropped, based on whether or not the interface is configured as part of a group.

In Junos OS, DHCP snooping is enabled in a routing instance when you configure either the dhcp-relay statement at the [edit forwarding-options] hierarchy level, or the dhcp-local-server statement at the [edit system services] hierarchy level in that routing instance. The router discards snooped packets by default if there is no subscriber associated with the packet. To enable normal processing of snooped packets, you must explicitly configure the allow-snooped-clients statement at the [edit forwarding-options dhcp-relay] hierarchy level.
You can configure DHCP snooping support for a specific routing instance for the following:

- **DHCPv4 relay agent**—Override the router’s (or switch’s) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets. A renew request may be unicast directly to the DHCP server. This is a BOOTREQUEST packet and is snooped.

- **DHCPv6 relay agent**—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- **DHCP local server**—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.

- You can also disable snooping filters. In the preceding configurations, all DHCP traffic is forwarded to the slower routing plane of the routing instance before it is either forwarded or dropped. Disabling snooping filters causes DHCP traffic that can be forwarded directly from the faster hardware control plane to bypass the routing control plane.

SEE ALSO

- *Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server*
- *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*
- *Disabling DHCP Snooping Filters*
- *Example: Enabling DHCP Snooping Support for DHCPv6 Relay Agent*
Example: Configuring DHCP Snooping Support for DHCP Relay Agent

This example shows how to configure DHCP snooping support for DHCP relay agent.

Requirements

• Configure DHCP relay agent. See “Extended DHCP Relay Agent Overview” on page 792.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

• Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group frankfurt.

• Configure DHCP relay agent to forward snooped packets to only configured interfaces.

NOTE: By default, DHCP snooping is disabled globally.

Configuration

Step-by-Step Procedure
To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.

   [edit]
   user@host# edit forwarding-options dhcp-relay
2. Specify the named group of interfaces on which DHCP snooping is supported.

```
[edit forwarding-options dhcp-relay]
user@host# edit group frankfurt
```

3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

4. Specify that you want to override the default configuration for the group.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# edit overrides
```

5. Enable DHCP snooping support for the group.

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# set allow-snooped-clients
```

6. Return to the `[edit forwarding-options dhcp-relay]` hierarchy level to configure the forwarding action and specify that DHCP relay agent forwards snooped packets on only configured interfaces:

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group `frankfurt`).

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```
Results
From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
    forward-snooped-clients configured-interfaces;
group frankfurt {
    overrides {
        allow-snooped-clients;
    }
    interface fe-1/0/1.3 {
        upto fe-1/0/1.9;
    }
}
}
```

If you are done configuring the device, enter `commit` from configuration mode.

SEE ALSO

* Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent

**Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent**

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the `forward-snooped-clients` statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, which is described in *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*, you enable or disable the DHCP relay snooping feature.

Table 56 on page 903 shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the `allow-snooped-clients` statement. Table 57 on page 903 shows the action the router (or
switch) takes on snooped packets when DHCP snooping is disabled by the `no-allow-snooped-clients` statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets. Table 58 on page 904 shows the action the router (or switch) takes for the snooped BOOTREPLY packets.

**NOTE:** Configured interfaces have been configured with the `group` statement in the `[edit forwarding-options dhcp-relay]` hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the `group` statement.

### Table 56: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled

<table>
<thead>
<tr>
<th><code>forward-snooped-clients</code> Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>forward-snooped-clients</code> not configured</td>
<td>snooped packets result in subscriber (DHCP client) creation</td>
<td>dropped</td>
</tr>
<tr>
<td><code>all-interfaces</code></td>
<td>forwarded</td>
<td>forwarded</td>
</tr>
<tr>
<td><code>configured-interfaces</code></td>
<td>forwarded</td>
<td>dropped</td>
</tr>
<tr>
<td><code>non-configured-interfaces</code></td>
<td>snooped packets result in subscriber (DHCP client) creation</td>
<td>forwarded</td>
</tr>
</tbody>
</table>

### Table 57: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled

<table>
<thead>
<tr>
<th><code>forward-snooped-clients</code> Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>forward-snooped-clients</code> not configured</td>
<td>dropped</td>
<td>dropped</td>
</tr>
<tr>
<td><code>all-interfaces</code></td>
<td>dropped</td>
<td>forwarded</td>
</tr>
<tr>
<td><code>configured-interfaces</code></td>
<td>dropped</td>
<td>dropped</td>
</tr>
<tr>
<td><code>non-configured-interfaces</code></td>
<td>dropped</td>
<td>forwarded</td>
</tr>
</tbody>
</table>
Table 58: Actions for Snooped BOOTREPLY Packets

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-snooped-clients not configured</td>
<td>snooped BOOTREPLY packets dropped if client is not found</td>
</tr>
<tr>
<td>forward-snooped-clients all configurations</td>
<td>snooped BOOTREPLY packets forwarded if client is not found</td>
</tr>
</tbody>
</table>

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.

   [edit]
   user@host# edit forwarding-options dhcp-relay

2. Enable DHCP snooped packet forwarding.

   [edit forwarding-options dhcp-relay]
   user@host# edit forward-snooped-clients

3. Specify the interfaces that are supported for snooped packet forwarding.

   [edit forwarding-options dhcp-relay forward-snooped-clients]
   user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

   [edit]
   forwarding-options {
     dhcp-relay {
       forward-snooped-clients configured-interfaces;
     }
   }

SEE ALSO
Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent
DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) can serve as a DHCP local server, a DHCP client, or a DHCP relay agent.

A Dynamic Host Configuration Protocol (DHCP) server can automatically allocate IP addresses and also deliver configuration settings to client hosts on a subnet. DHCP lets network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network. An IP address can be leased to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses among a group of hosts that do not need permanent IP addresses.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts, such as PCs, that are connected to device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network.

The device can also operate as a DHCP client and DHCP relay agent.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.

NOTE: Although a Juniper Networks device can act as a DHCP server, a DHCP client, or DHCP relay agent at the same time, you cannot configure more than one DHCP role on a single interface.

DHCP provides two primary functions:

- Allocate temporary or permanent IP addresses to clients.
- Store, manage, and provide client configuration parameters.

NOTE: On all SRX Series devices, DHCPv4 is supported only in Layer 3 mode; the DHCP server and DHCP client are not supported in Layer 2 transparent mode.
DHCP Local Server

You can enable an SRX Series device to function as a DHCP local server, and then configure its options on the device. The DHCP local server provides an IP address and other configuration information in response to a client request.

To configure the DHCP local server on the device, include the `dhcp-local-server` statement at the `[edit system services]` hierarchy level.

**NOTE:** You cannot configure the DHCP local server and the DHCP relay agent on the same interface.

DHCP Client, DHCP Local Server, and Address-Assignment Pool Interaction

In a typical branch network configuration, the DHCP client is on the subscriber’s computer, and the DHCP local server is configured on the device. The following steps provide a high-level description of the interaction among the DHCP client, DHCP local server, and address-assignment pools.

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server and client installs the host route and ARP entry, and then monitors the lease state.

DHCP Local Server and Address-Assignment Pools

In a DHCP local server operation, the client address and configuration information reside in centralized address-assignment pools, that are managed independently from the DHCP local server and they can be shared by different client applications.
Configuring a DHCP environment that includes a DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the DHCP local server on the device and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

**NOTE:** The DHCP local server and the address-assignment pools used by the server must be configured in the same routing instance.

### DHCP Client

DHCP configuration consists of configuring DHCP clients and a DHCP local server. A client configuration determines how clients send a message requesting an IP address, while a server configuration enables the server to send an IP address back to the client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval.

### DHCP Relay Agent

You can configure DHCP relay options on the device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP local server.

To configure the DHCP relay agent on the router, include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level.

You can also include the `dhcp-relay` statement at the following hierarchy level:

`[edit routing-instances routing-instance-name forwarding-options]`
DHCP Client, DHCP Relay Agent, and DHCP Local Servers

In a typical branch network configuration, the DHCP client is on the subscriber’s computer, and the DHCP relay agent is configured on the device between the DHCP client and one or more DHCP local servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP local server interact in a configuration that includes two DHCP local servers.

1. The DHCP client sends a discover packet to find a DHCP local server in the network from which to obtain configuration parameters for the subscriber, including an IP address.

2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP local servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client’s state.

3. In response to receiving the discover packet, each DHCP local server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.

4. On receipt of the offer packets, the DHCP client selects the DHCP local server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.

5. The DHCP client sends a request packet that specifies the DHCP local server from which to obtain configuration information.

6. The DHCP local server requested by the client sends an acknowledgement (ACK) packet that contains the client’s configuration parameters.

7. The DHCP relay agent receives the ACK packet and forwards it to the client.

8. The DHCP client receives the ACK packet and stores the configuration information.

9. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.

10. After establishing the initial lease on the IP address, the DHCP client and the DHCP local server use unicast transmission to negotiate lease renewal or release.
Considerations

The following considerations apply when you enable a DHCP local server, DHCP relay agent, or DHCP client in a routing instance:

- The DHCP local server, DHCP relay agent, and DHCP client can be configured in one routing instance, but the functionality is mutually exclusive on one interface. If the DHCP client is enabled on one interface, the DHCP local server or the DHCP relay agent cannot be enabled on that interface.

- The DHCP client, DHCP relay agent and DHCP local server services act independently in their respective routing instance. The following features can function simultaneously on a device:
  - DHCP client and DHCP local server
  - DHCP client and DHCP relay agent
  - Multiple routing instances. Each instance can have a DHCP local server, DHCP relay agent, or DHCP client, or each routing instance can have a DHCP client and DHCP local server or a DHCP client and DHCP relay agent.

- In Junos Release 12.1X46, autoinstallation is not compatible with jDHCPd:

```shell
version 12.1X46-D40.2;
system {
    /* not compatible with jDHCPd */ <<<<<<
    autoinstallation {
        usb {
            disable;
        }
    }
}
```

**NOTE:** Before you enable DHCP services in a routing instance, you must remove all the configuration related to DHCP services that does not include routing instance support. If you do not do this, the old default routing instance configuration will override the new routing instance configuration.

**NOTE:** On all SRX Series devices, logical systems and routing instances are not supported for a DHCP client in chassis cluster mode.
DHCP Settings and Restrictions Overview

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP’s DHCP name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device’s internal network.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the `show system services dhcp conflict` command. The addresses in the conflicts list remain excluded until you use the `clear system services dhcp conflict` command to manually clear the list.

DHCP Interface Restrictions

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types.

DHCP is not supported on interfaces that are part of a virtual private network (VPN).

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Understanding DHCP Server Operation</th>
<th>915</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding DHCP Client Operation</td>
<td>933</td>
</tr>
<tr>
<td>Understanding DHCP Relay Agent Operation</td>
<td>945</td>
</tr>
</tbody>
</table>
A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A device acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network. Read this topic for more information.

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. Juniper Networks devices can
also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

This section contains the following topics:

**DHCP Options**

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

**Compatibility with Autoinstallation**

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

**Chassis Cluster Support**

DHCP server operations are supported on all SRX Series devices in chassis cluster mode.

**SEE ALSO**

- DHCP Overview | 909
- Understanding DHCP Client Operation | 933
- Understanding DHCP Relay Agent Operation | 945

**DHCP Server Configuration Overview**

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device interface:
- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.
- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.
- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. Table 59 on page 917 provides the settings and values for the sample DHCP server configuration.

Table 59: Sample DHCP Server Configuration Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Subnet Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Address pool subnet address</td>
<td>192.168.2.0/24</td>
</tr>
<tr>
<td>High address in the pool range</td>
<td>192.168.2.254</td>
</tr>
<tr>
<td>Low address in the pool range</td>
<td>192.168.2.2</td>
</tr>
<tr>
<td>Address pool default lease time, in seconds</td>
<td>1,209,600 (14 days)</td>
</tr>
<tr>
<td>Address pool maximum lease time, in seconds</td>
<td>2,419,200 (28 days)</td>
</tr>
<tr>
<td>Domain search suffixes</td>
<td>mycompany.net</td>
</tr>
<tr>
<td></td>
<td>mylab.net</td>
</tr>
<tr>
<td>Address to exclude from the pool</td>
<td>192.168.2.33</td>
</tr>
<tr>
<td>DNS server address</td>
<td>192.168.10.2</td>
</tr>
<tr>
<td>Identifier code for router solicitation address option</td>
<td>32</td>
</tr>
<tr>
<td>Type choice for router solicitation address option</td>
<td>Ip address</td>
</tr>
<tr>
<td>IP address for router solicitation address option</td>
<td>192.168.2.33</td>
</tr>
<tr>
<td><strong>DHCP MAC Address Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Static binding MAC address</td>
<td>01:03:05:07:09:0B</td>
</tr>
</tbody>
</table>
Minimum DHCP Local Server Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP local server. In this output, the server group is named mobileusers, and the DHCP local server is enabled on interface ge-1/0/1.0 within the group. The address pool is named acmenetwork from low range of 192.168.1.10/24 to a high range of 192.168.1.20/24.

```
[edit access]
  address-assignment {
    pool acmenetwork {
      family inet {
        network 192.168.1.0/24;
        range r1 {
          low 192.168.1.10;
          high 192.168.1.20;
        }
      }
    }
  }

edit system services
dhcp-local-server {
  group mobileusers {
```

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed address</td>
<td>192.168.2.50</td>
</tr>
</tbody>
</table>

SEE ALSO

- DHCP Overview | 909
- Understanding DHCP Client Operation | 933
- Understanding DHCP Relay Agent Operation | 945
- RFC 3397, Dynamic Host Configuration Protocol (DHCP) Domain Search Option
interface ge-1/0/1.0
}
}

edit interfaces ge-1/0/1 unit 0
family {
    inet {
        address 192.168.1.1/24
    }
}

NOTE: You can configure the DHCP local server in a routing instance by using the dhcp-local server, interface, and address-assignment statements in the [edit routing-instances] hierarchy level.

SEE ALSO

Configuring Address-Assignment Pools | 929

Enabling TCP/IP Propagation on a DHCP Local Server

This topic describes how to configure TCP/IP settings on a DHCP local server, which includes a DHCP client and a DHCP local server.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

To enable TCP/IP setting propagation on a DHCP local server:

1. Configure the update-server option on the DHCP client.

[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp-client {
    update-server;
2. Configure the address pool to specify the interface (where `update-server` is configured) from which TCP/IP settings can be propagated.

```plaintext
[edit access]
address-assignment {
    pool sprint family inet {
        network 192.168.2.0/24;
        dhcp-attributes {
            propagate-settings ge-0/0/1.0;
        }
    }
}
```

3. Configure the DHCP local server.

```plaintext
edit system services
dhcp-local-server {
    group bob {
        interface ge-1/0/1.0
    }
}
```

SEE ALSO

- Minimum DHCP Local Server Configuration | 918

| Example: Configuring the Device as a DHCP Server |

IN THIS SECTION

- Requirements | 921
- Overview | 921
This example shows how to configure the device as a DHCP server.

For information on how to configure JDHCP in a routing instance, see How to configure JDHCP in a routing instance.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the Understanding Management Predefined Policy Applications.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the maximum-lease-time to 2,419,200. Then you specify the DNS server IP address as 192.168.10.2.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated. and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.
Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the set access hierarchy level, and then enter commit from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
set system services dhcp-local-server group g1 interface ge-0/0/2.0
set access address-assignment pool p1 family inet network 192.168.2.0/24
set access address-assignment pool p1 family inet range r1 low 192.168.2.2
set access address-assignment pool p1 family inet range r1 high 192.168.2.254
set access address-assignment pool p1 family inet dhcp-attributes maximum-lease-time 2419200
set access address-assignment pool p1 family inet dhcp-attributes name-server 192.168.10.2
```

GUI Step-by-Step Procedure
To configure the device as a DHCP server, specify the DHCP pool information, server information, lease time, and option information:

1. In the J-Web interface, select Configure > DHCP > DHCP Services.

2. Select DHCP Pools. Click Add.

3. Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.

4. Specify the subnet information for the IPv4 address-assignment pool. Type 192.168.2.0/24.

5. In the Address Range Low, type 192.168.2.2.

6. In the Address Range High, type 192.168.2.254.

7. In the Exclude Addresses box, type the addresses you want excluded from a DHCP address pool. Type 192.168.2.0/24

8. Specify the server identifier to assign to any DHCP clients in this address pool. The identifier can be used to identify a DHCP server in a DHCP message.

9. Specify the domain name to assign to any DHCP clients in this address pool.

10. Specify the next server that DHCP clients need to contact. Type 192.168.10.2
11. Define the maximum amount of time (in seconds) that DHCP should lease an address. Type 2419200.

12. Define DHCP option 32, the device solicitation address option. You must enter a numeric value for option code. Select the option type from the list that corresponds to the option code.

13. Click OK.

14. If you are done configuring the device, click Commit > Commit.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure the device as a DHCP server:

1. Configure an interface with an IP address on which the DHCP server will be reachable.

   ```
   [edit]
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
   ```

2. Configure the DHCP server.

   ```
   [edit]
   user@host# set system services dhcp-local-server group g1 interface ge-0/0/2.0
   ```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

   ```
   [edit]
   user@host# set access address-assignment pool p1 family inet network 192.168.2.0/24
   ```

4. (Optional) Specify the IP address pool range. Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

   ```
   [edit]
   user@host# set access address-assignment pool p1 192.168.2.0/24 address-range low 192.168.2.2 high 192.168.2.254
   ```
5. (Optional) Configure one or more routers as the default gateway on the client's subnet.

```
[edit]
user@host# set access address-assignment pool p1 family inet dhcp-attributes router 192.168.10.3
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes server-identifier 192.168.10.1
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes maximum-lease-time 2419200
```

8. (Optional) Specify user-defined options to be included in DHCP packets

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes option 98 string test98
```

9. Assign a fixed IP address with the MAC address of the client.

```
[edit]
user@host# set access address-assignment pool pool1 family inet host host1 ip-address 192.168.2.100 hardware-address 2c:56:dc:72:99:f3
```

**Results**

- From configuration mode, confirm your configuration by entering the `show access address-assignment` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access address-assignment
pool p1 {
```
family inet {
  network 192.168.2.0/24;
  range r1 {
    low 192.168.2.2;
    high 192.168.2.254;
  }
  dhcp-attributes {
    maximum-lease-time 2419200;
    name-server {
      192.168.10.2;
    }
  }
}

• From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
```

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

**IN THIS SECTION**

- Verifying the DHCP Binding Database | 925
- Verifying DHCP Server Operation | 926

Confirm that the configuration is working properly.

**Verifying the DHCP Binding Database**

**Purpose**
Verify that the DHCP binding database reflects the DHCP server configuration.

**Action**

From operational mode, enter these commands:

- **show dhcp server binding** command to display all active bindings in the database.
- **show dhcp server binding address detail** command (where *address* is the IP address of the client) to display more information about a client.

These commands produce following sample output:

```
user@host> show dhcp server binding

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hardware Address</th>
<th>Type</th>
<th>Lease expires at</th>
</tr>
</thead>
</table>

user@host> show dhcp server binding address detail
```

```
| IP address           | 192.0.2.2          |
| Hardware address     | 00:a0:12:00:13:02  |
| Pool                 | 192.0.2.0/24       |
| Interface            | fe-0/0/0, relayed by 192.0.2.200 |

Lease information:
- Type: DHCP
- Obtained at: 2004-05-02 13:01:42 PDT
- Expires at: 2004-05-03 13:01:42 PDT
- State: active

DHCP options:
- Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
- Name: domain-name, Value: mydomain.tld
- Code: 32, Type: ip-address, Value: 192.0.2.33
```

**Verifying DHCP Server Operation**

**Purpose**

Verify that the DHCP server operation has been configured.

**Action**

From operational mode, enter the following command:
• `show dhcp server statistics` command to verify the DHCP server statistics.

```
user@host> show dhcp server statistics
```

<table>
<thead>
<tr>
<th>Packets dropped:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages received:</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREQUEST</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
</tr>
<tr>
<td>DHCPDISCOVER</td>
</tr>
<tr>
<td>DHCPINFORM</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
</tr>
<tr>
<td>DHCPLEASEQUERY</td>
</tr>
<tr>
<td>DHCPBULKLEASEQUERY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages sent:</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREPLY</td>
</tr>
<tr>
<td>DHCPOFFER</td>
</tr>
<tr>
<td>DHCPACK</td>
</tr>
<tr>
<td>DHCPNAK</td>
</tr>
<tr>
<td>DHCPFORCERENEW</td>
</tr>
<tr>
<td>DHCPLEASEUNASSIGNED</td>
</tr>
<tr>
<td>DHCPLEASEUNKNOWN</td>
</tr>
<tr>
<td>DHCPLEASEACTIVE</td>
</tr>
<tr>
<td>DHCPLEASEQUERYDONE</td>
</tr>
</tbody>
</table>

**SEE ALSO**

- DHCP Overview  | 909
- Understanding DHCP Relay Agent Operation  | 945

**Verifying and Managing DHCP Local Server Configuration**

**Purpose**

View or clear information about client address bindings and statistics for the extended DHCP local server.
NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the clear dhcp server binding command before you delete the DHCP server configuration.

Action

- To display the address bindings in the client table on the extended DHCP local server:
  ```
  user@host> show dhcp server binding routing-instance customer routing instance
  ```

- To display extended DHCP local server statistics:
  ```
  user@host> show dhcp server statistics routing-instance customer routing instance
  ```

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:
  ```
  user@host> clear dhcp server binding routing-instance customer routing instance
  ```

- To clear all extended DHCP local server statistics:
  ```
  user@host> clear dhcp server statistics routing-instance customer routing instance
  ```

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D60</td>
<td>Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CL is supported.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- DHCP Address-Assignment Pools | 929
- DHCP Client | 933
- DHCP Relay Agent | 944
- DHCPv6 Server | 962
Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address. For more information, read this topic.

### Configuring Address-Assignment Pools

The address-assignment pool feature for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices enables you to create address pools that can be shared by different client applications such as DHCPv4 or DHCPv6.

To configure an address-assignment pool:

1. Configure the address-assignment pool name and specify the addresses for the pool.
   
   See "Configuring an Address-Assignment Pool Name and Addresses" on page 930.

2. (Optional) Configure named ranges (subsets) of addresses.
   
   See "Configuring a Named Address Range for Dynamic Address Assignment" on page 930.

3. (Optional;IPv4 only) Create static address bindings.
   
   See "Configuring Static Address Assignments" on page 931.

4. (Optional) Configure attributes for DHCP clients.
   
   See "Configuring DHCP Client-Specific Attributes for Address-Assignment Pools" on page 934.
**Configuring an Address-Assignment Pool Name and Addresses**

When configuring an address-assignment pool on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices, you must specify the name of the pool and its addresses.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.
   
   ```
   [edit access]
   user@host# edit address-assignment pool blr-pool family inet
   ```

2. Configure the network address and the prefix length of the addresses in the pool.
   
   ```
   [edit access address-assignment pool blr-pool family inet]
   user@host# set network 192.168.0.0/16
   ```

   **NOTE:** You can configure an IPv4 address-assignment pool in a routing instance by configuring the address-assignment statements at the `[edit routing-instance routing-instance-name]` hierarchy level. For example `[edit routing-instances routing-instances name access address-assignment pool blr-pool family inet]`. The above steps shows only the `[edit access]` configuration.

**Configuring a Named Address Range for Dynamic Address Assignment**

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During a dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

**NOTE:** Supported only on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool.
   
   ```
   [edit access]
   ```
2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```bash
[edit access address-assignment pool isp_1 family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```

**NOTE:** To configure named address ranges in a routing instance, configure the address-assignment statements in the [edit routing-instances] hierarchy level.

### Configuring Static Address Assignments

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address.

**NOTE:** This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

To configure a static IPv4 address binding:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```bash
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 01:03:05:07:09:0b is always assigned IP address 192.168.10.2.

```bash
[edit access address-assignment pool blr-pool family inet]
```
NOTE: To configure static binding for an IPv4 address in a routing instance, configure the `address-assignment` statements in the `[edit routing-instances]` hierarchy.

## Configuring Address-Assignment Pool Linking

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example, you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the device switches to pool B for addresses. When pool B is exhausted, the device switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool.

To link a primary address-assignment pool named `pool1` to a secondary pool named `pool2` on SRX1500, SRX5400, SRX5600, or SRX5800 devices:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```
DHCP Client

IN THIS SECTION

- Understanding DHCP Client Operation | 933
- Minimum DHCP Client Configuration | 934
- Configuring DHCP Client-Specific Attributes for Address-Assignment Pools | 934
- Configuring Optional DHCP Client Attributes | 935
- Verifying and Managing DHCP Client Configuration | 936
- Example: Configuring the Device as a DHCP Client | 937

SRX Series device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. For more information, read this topic.

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series devices in chassis cluster mode.

SEE ALSO

- DHCP Overview | 909
- Understanding DHCP Relay Agent Operation | 945
Minimum DHCP Client Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family inet {
      dhcp-client
    }
  }
}
```

**NOTE:** To configure a DHCP client in a routing instance, add the interface in a routing instance using the [edit routing-instances] hierarchy.

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot file that the client uses, the DNS server, and the maximum lease time.

**NOTE:** This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

You use the dhcp-attributes statement to configure DHCP client-specific attributes for address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name of the address-assignment pool.
2. Configure optional DHCP client attributes.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

```
[edit access address-assignment pool blr-pool family inet]
user@host# set dhcp-attributes maximum-lease-time 2419200
user@host# set dhcp-attributes name-server 192.168.10.2
user@host# set dhcp-attributes boot-file boot-file.txt
user@host# set dhcp-attributes boot-file boot-server example.com
```

**NOTE:** To configure DHCP client-specific attributes in a routing instance, configure the `dhcp-attributes` statements in the `[edit routing-instances]` hierarchy.

---

### Configuring Optional DHCP Client Attributes

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```
3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

NOTE: To configure the DHCP client in a routing instance, configure the interface in the `[edit routing-instances]` hierarchy.

---

### Verifying and Managing DHCP Client Configuration

**Purpose**

View or clear information about client address bindings and statistics for the DHCP client on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.
### Action

- To display the address bindings in the client table on the DHCP client:

  ```bash
  user@host> show dhcp client binding
  ```

- To display DHCP client statistics:

  ```bash
  user@host> show dhcp client statistics
  ```

- To clear the binding state of a DHCP client from the client table on the DHCP client:

  ```bash
  user@host> clear dhcp client binding
  ```

- To clear all DHCP client statistics:

  ```bash
  user@host> clear dhcp client statistics
  ```

**NOTE:** To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp client binding routing instance <routing-instance name>`
- `show dhcp client statistics routing instance <routing-instance name>`
- `clear dhcp client binding routing instance <routing-instance name>`
- `clear dhcp client statistics routing instance <routing-instance name>`

### Example: Configuring the Device as a DHCP Client

**IN THIS SECTION**

- Requirements | 938
- Overview | 938
- Configuration | 939
- Verification | 942
This example shows how to configure the device as a DHCP client.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. You can use the `show system services dhcp pool` CLI command to view information on DHCP address pools.

- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.

- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.

- Determine the DHCP options required by the subnets and clients in your network. See "Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server" on page 707

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/2, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 50,000, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Set the force-discover option if you want to force the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.
WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

NOTE: Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-client at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to align with other Junos platforms. There is no change in the functionality.

Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet dhcp-client client-identifier prefix host-name
set interfaces ge-0/0/2 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/2 unit 0 family inet dhcp-client force-discover
set interfaces ge-0/0/2 unit 0 family inet dhcp-client server-address 192.168.2.1
set interfaces ge-0/0/2 unit 0 family inet dhcp-client vendor-id ether
set interfaces ge-0/0/2 unit 0 family inet dhcp-client options no-hostname
```

GUI Step-by-Step Procedure
To configure the device as a DHCP client:

1. In the J-Web interface, select Configure > Services > DHCP > DHCP Client.

2. Under Interfaces, add ge-0/0/2.0.
3. Configure the DHCP client identifier as either an ASCII or hexadecimal value.

4. From the Client identifier choice list, select hexadecimal.

5. In the Hexadecimal box, type the client identifier—00:0a:12:00:12:12.

6. Set the DHCP lease time in seconds. This is the lease time in seconds requested in a DHCP client protocol packet; the range is 60 through 2,147,483,647. Type 86400.

7. Set the retransmission number of attempts to 6. This is the number of attempts to retransmit the DHCP client protocol packet. The range is 0 through 6.

8. Set the retransmission interval in seconds to 5. This is the number of seconds between successive transmissions. The range is 4 through 64. The default is 4 seconds.

9. Configure the force-discover option to force the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts.

10. Set the IPv4 address of the preferred DHCP server. Type 192.168.2.1.

11. Set the vendor class ID. This is the vendor class identification for the DHCP client. Type ether.

12. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).

13. Click OK.

14. If you are done configuring the device, click Commit >.

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

   ```plaintext
   [edit]
   user@host# edit interfaces ge-0/0/2 unit 0 family inet dhcp-client
   ```

2. Configure the DHCP client identifier as a hexadecimal value.
3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Configure the force-discover option.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set force-discover.
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set server-address 192.168.2.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

9. Configure options no-hostname if you do not want the client to send the hostname in packets.
Results
From configuration mode, confirm your configuration by entering the `show interfaces ge-0/0/2 unit 0 family inet dhcp-client` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/2 unit 0 family inet
dhcp-client {
    client-identifier hexadecimal 00:0a:12:00:12:12;
    options no-hostname;
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    force-discover;
    server-address 192.168.2.1;
    update-server;
    vendor-id ether;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Client | 942

Confirm that the configuration is working properly.

Verifying the DHCP Client

Purpose
Verify that the DHCP client information has been configured.

Action
From operational mode, enter these commands:

- **show dhcp client binding** command to display the binding state of a Dynamic Host Configuration Protocol (DHCP) client.

- **show dhcp client statistics** command to display client statistics.

These commands produce the following sample output:

```
user@host> show dhcp client binding

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.2</td>
<td>88:a2:5e:0a:d6:03</td>
<td>2419093</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
</tbody>
</table>

user@host> show dhcp client statistics

Packets dropped:
  Total    2
  Send error  2

Messages received:
  BOOTREPLY  6
  DHCPOFFER  4
  DHCPACK    2
  DHCPNAK    0
  DHCPFORCERENEW  0

Messages sent:
  BOOTREQUEST    39
  DHCPDECLINE    0
  DHCPDISCOVER   23
  DHCPREQUEST    16
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPRENEW      0
  DHCPREBIND     0
```

SEE ALSO
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to align with other Junos platforms.

Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported.
The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks. For more information, read this topic.

### Understanding DHCP Relay Agent Operation

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

**NOTE:** The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces <interface name> unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

See ALSO

| DHCP Overview | 909 |
| Understanding DHCP Server Operation | 915 |

### Example: Minimum JDHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```conf
[edit forwarding-options]
dhcp-relay {
    server-group {
        test 203.0.113.21;
    }
}
```
active-server-group test;
group all {
    interface fe-0/0/2.0;
}

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates a server group and an active server group named test with IP address 203.0.113.21. The DHCP relay agent configuration is applied to a group named all. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Example: Configuring JDHCP Relay Configuration

IN THIS SECTION
- Requirements | 947
- Overview | 947
- Configuration | 948
- Verification | 955

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

This example describes how to configure the DHCP relay agent on the SRX Series device. SRX series device acting as DHCP relay agent is responsible for forwarding the requests and responses between the DHCP clients and the server which are part of different routing instances.
Requirements

This example uses the following hardware and software components:

- SRX Series devices with Junos OS 15.1X49-D10 or later.

Overview

You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that is isolated from the client network.

Topology

To exchange DHCP messages between different routing instances, you must enable both the server-facing interface and the client-facing interface of the DHCP relay agent to recognize and forward DHCP packets.

The following Figure 43 on page 947 shows DHCP performance as DHCP local server, DHCP client, and DHCP relay agent

Figure 43: Understanding DHCP Services in a Routing Instance

The following list provides an overview of the tasks required to create the DHCP message exchange between the different routing instances:

- Configure the client-facing side of the DHCP relay agent.
- Configure the server-facing side of the DHCP relay agent.
- Configure the Security Zone to Allow the DHCP protocol.

Table 1: DHCP Relay Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Client-Side-Details</th>
<th>Server-Side-Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>ge-0/0/3.0</td>
<td>ge-0/0/3.0</td>
</tr>
<tr>
<td>routing interface</td>
<td>trust-vr</td>
<td>untrust-vr</td>
</tr>
</tbody>
</table>
### Configuration

**CLI Quick Configuration**

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different routing instances. To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter `commit` from configuration mode.

**Quick configuration for Client-Facing Support:**

```
set routing-instances trust-vr instance-type virtual-router
set routing-instances trust-vr interface ge-0/0/3.0
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

**Quick configuration for Server-Facing Support:**

```
set routing-instances untrust-vr instance-type virtual-router
set routing-instances untrust-vr interface ge-0/0/4.0
set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

**Quick configuration for DHCP Relay Support:**

```
set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-config
set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
```
Quick configuration for Security Zone to Allow the DHCP Protocol:

```text
set security policies default-policy permit-all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic protocols all
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure support on the client-facing side of the DHCP relay agent:

1. Set a routing instance type as virtual router.

   ```text
   [edit]
   user@host# set routing-instances trust-vr instance-type virtual-router
   ```

2. Set an interface to the virtual router

   ```text
   [edit]
   user@host# set routing-instances trust-vr interface ge-0/0/3.0
   ```

3. Set the IP address to the interface.

   ```text
   [edit]
   ```
Step-by-Step Procedure
To configure support on the server-facing side of the DHCP relay agent:

1. Set a virtual router.

   ```
   [edit]
   user@host# set routing-instances untrust-vr instance-type virtual-router
   ```

2. Set an interface to the virtual router.

   ```
   [edit]
   user@host# set routing-instances untrust-vr interface ge-0/0/4.0
   ```

3. Set the forward-only-replies option.

   ```
   [edit]
   user@host# set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
   ```

4. Set the IP address to the interface.

   ```
   [edit]
   user@host# set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
   ```

Step-by-Step Procedure
To configure the DHCP local server to support:

1. Set the configuration in dhcp-relay for untrust-vr routing instance

   ```
   [edit ]
   user@host# set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-config
   user@host# set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
   user@host# set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
   ```

2. Set the configuration in dhcp-relay for trust-vr routing instance

   ```
   [edit ]
   ```
user@host# set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1 30.1.1.2
user@host# set routing-instances trust-vr forwarding-options dhcp-relay active-server-group server-1
user@host# set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr interface ge-0/0/3.0
user@host# set routing-instances trust-vr routing-options instance-import export_dhcp_server_route

3. Set the configuration to share routes between routing instances.

[edit ]
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from instance untrust-vr
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from route-filter
    30.1.1.0/24 exact
user@host# set policy-options policy-statement export_dhcp_server_route term 1 then accept
user@host# set policy-options policy-statement export_dhcp_server_route term 2 then reject
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance trust-vr
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter
    10.1.1.0/24 exact
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 2 then reject
user@host# set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0

NOTE: You can enable an SRX Series device to function as a DHCP local server. The DHCP local server provides an IP address and other configuration information in response to a client request.

Step-by-Step Procedure
To configure the security zone to allow the DHCP Protocol:

1. Set the default security policy to permit all traffic.

[edit ]
user@host# set security policies default-policy permit-all

2. Set all system services and protocols on interface ge-0/0/4.0.

[edit ]
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic
    system-services all
3. Set all system services and protocols on interface ge-0/0/3.0.

Results

- Result for Client-facing Support:

From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

- Result for Server-Facing Support:

From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.
• Result for DHCP Local Server Support:

From configuration mode, confirm your configuration by entering the `show routing-instances`, `show policy-options` and `show routing-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
  routing-options {
    instance-import export_dhcp_server_route;
  }
  forwarding-options {
    dhcp-relay {
      server-group {
        server-1 {
          30.1.1.2;
        }
      }
      active-server-group server-1;
      group relay-in-vr {
        interface ge-0/0/3.0;
      }
    }
  }
}

untrust-vr {
  routing-options {
    static {
      route 30.1.1.0/24 next-hop 20.1.1.2;
    }
    instance-import import_relay_route_to_server_vr;
  }
  forwarding-options {
    dhcp-relay {
      server-group {
        dummy-config;
      }
    }
  }
}
[edit]
user@host# show policy-options
policy-statement export_dhcp_server_route {
  term 1 {
```
from {
    instance untrust-vr;
    route-filter 30.1.1.0/24 exact;
}
    then accept;
} term 2 {
    then reject;
}
}
policy-statement import_relay_route_to_server_vr {
    term 1 {
        from {
            instance trust-vr;
            route-filter 10.1.1.0/24 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}

[edit]
user@host# show routing-options
static {
    route 30.1.1.2/32 next-table untrust-vr.inet.0;
}

- Result for Security Zone to Allow the DHCP Protocol:

From configuration mode, confirm your configuration by entering the show security policies and show security zones commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security zones
security-zone HOST {
    interfaces {
        all;
    }
If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

Confirm that the configuration is working properly.

**Verifying the DHCP Relay Statistics Configuration:**

**Purpose**
Verify that the DHCP Relay Statistics has been configured.

**Action**
- From operational mode, enter the `show dhcp relay statistics routing-instance dhcp-relay` command.
Packets dropped:
Total 0

Messages received:
BOOTREQUEST 1
DHCPDECLINE 0
DHCPDISCOVER 0
DHCPINFORM 0
DHCPRELEASE 0
DHCPREQUEST 1

Messages sent:
BOOTREPLY 1
DHCPOFFER 0
DHCPACK 1
DHCPNAK 0
DHCPFORCERENEW 0

Verifying DHCP client bindings in the routing instance.

Purpose
Verify that the DHCP client bindings in the routing instances has been configured.

Action
• From operational mode, enter the `show dhcp relay binding routing-instance dhcp-relay` command.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Session Id</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.2</td>
<td>14</td>
<td>00:0c:29:e9:6d:00</td>
<td>86381</td>
<td>BOUND</td>
<td>ge-0/0/1.0</td>
</tr>
</tbody>
</table>

Example: Configuring the Device as a BOOTP or DHCP Relay Agent using Legacy DHCP Deamon Command
This example shows how to configure the device as a BOOTP or DHCP relay agent.

**Requirements**

No special configuration beyond device initialization is required before configuring this feature.

**Overview**

In this example, you enable the DHCP relay agent to relay BOOTP or DHCP messages to a BOOTP server. You specify the IP time-to-live value to be set in responses to the client as 20. The range is from 1 through 255. You then set the maximum number of hops allowed per packet to 10. The range is from 1 through 16.

Then you specify the minimum number of seconds before requests are forwarded as 300. The range is from 0 through 30,000 seconds.

You then specify the IP time-to-live value to be set in responses to the client as 30. The range is from 1 through 255. You set the description of the server as text and the DHCP option as 82. You set the maximum number of hops allowed per packet to 16 and specify the minimum number of seconds as 400 before requests are forwarded.

**WARNING:** Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

**WARNING:** The DHCP configuration command used will be deprecated in future Junos releases.

**WARNING:** Please see documentation for updated commands.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set forwarding-options helpers bootp client-response-ttl 20
set forwarding-options helpers bootp maximum-hop-count 10
```
set forwarding-options helpers bootp minimum-wait-time 300
set forwarding-options helpers bootp description text
set forwarding-options helpers bootp interface ge-0/0/0 client-response-ttl 30
set forwarding-options helpers bootp interface ge-0/0/0 description text
set forwarding-options helpers bootp interface ge-0/0/0 dhcp-option82
set forwarding-options helpers bootp interface ge-0/0/0 maximum-hop-count 16
set forwarding-options helpers bootp interface ge-0/0/0 minimum-wait-time 400

GUI Step-by-Step Procedure
To configure the device as a BOOTP/DHCP relay agent:

1. In the Client response TTL box, type 20.
2. In the Maximum hop count box, type 10.
3. In the Minimum wait time box, type 300.
4. In the Description box, type the description of the server.
5. In the Client response TTL box, type 30.
6. In the Description box, type the description of the server.
7. Select the Dhcp option 82 check box.
8. In the Maximum hop count box, type 16.
9. In the Minimum wait time box, type 400.
10. Click OK until you return to the Configuration page.
11. Click OK to check your configuration and save it as a candidate configuration.
12. If you are done configuring the device, click Commit Options>Commit.

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the device as a BOOTP or DHCP relay agent:

1. Specify the IP time-to-live value in BOOTP response messages sent to a BOOTP client.

   ```
   [edit forwarding-options helpers bootp]
   user@host# set client-response-ttl 20
   ```

2. Specify the maximum number of hops allowed per packet.

   ```
   [edit forwarding-options helpers bootp]
   user@host# set maximum-hop-count 10
   ```

3. Specify the minimum wait time in seconds.

   ```
   [edit forwarding-options helpers bootp]
   user@host# set minimum-wait-time 300
   ```

4. Specify the description of the server.

   ```
   [edit forwarding-options helpers bootp]
   user@host# set description text
   ```

5. Define the incoming BootP request forwarding interface.

   ```
   [edit forwarding-options helpers bootp]
   user@host# set interface ge-0/0/0
   ```

6. Define the IP time-to-live value.

   ```
   [edit forwarding-options helpers bootp interface ge-0/0/0]
   user@host# set client-response-ttl 30
   ```

7. Specify the description of the server.

   ```
   [edit forwarding-options helpers bootp interface ge-0/0/0]
   user@host# set description text
   ```
8. Set the DHCP option 82.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set dhcp-option82
```

9. Specify the maximum number of hops allowed per packet.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set forwarding-options helpers bootp interface ge-0/0/0 maximum-hop-count 16
```

10. Specify the minimum wait time.

```
[edit forwarding-options helpers bootp interface ge-0/0/0]
user@host# set minimum-wait-time 400
```

**Results**

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show forwarding-options
helpers {
  bootp {
    description text;
    maximum-hop-count 10;
    minimum-wait-time 300;
    client-response-ttl 20;
    interface {
      ge-0/0/0 {
        description text;
        maximum-hop-count 16;
        minimum-wait-time 400;
        client-response-ttl 30;
        dhcp-option82;
      }
    }
  }
}
```

If you are done configuring the device, enter commit from configuration mode.
Verification

Confirm that the configuration is working properly.

Verifying DHCP Relay Statistics

Purpose

Verify that the DHCP Relay statistics have been configured.

Action

From operational mode, enter the `show system services dhcp relay-statistics` command.

```
user@host> show system services dhcp relay-statistics
```

<table>
<thead>
<tr>
<th>Received Packets:</th>
<th>4</th>
<th>Forwarded Packets</th>
<th>4</th>
<th>Dropped Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>Due to missing interface in relay database:</td>
<td>4</td>
<td>Due to missing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>matching routing instance:</td>
<td></td>
<td>matching routing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Due to an error during packet read:</td>
<td></td>
<td>instance:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Due to an error during packet send:</td>
<td></td>
<td>Due to an error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Due to invalid server address:</td>
<td></td>
<td>during packet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Due to missing valid local address:</td>
<td></td>
<td>send:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Due to missing route to server/client:</td>
<td></td>
<td>invalid server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>Due to missing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>valid local</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>route to server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>/client:</td>
</tr>
</tbody>
</table>

SEE ALSO

**DHCP Overview** | 909

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D60</td>
<td>Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

**DHCP Server** | 915  
**DHCP Address-Assignment Pools** | 929  
**DHCP Client** | 933
SRX Series device can act as a DHCPv6 server and allocates IP addresses to IPv6 clients. DHCPv6 server also delivers configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. For more information, read this topic.

### DHCPv6 Server Overview

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IPv6 clients and deliver configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. A DHCPv6 server allows network administrators to manage pool of IP addresses centrally among hosts and to automate the assignment of IP addresses in a network.

**NOTE:** SRX Series devices do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)
- Prefix delegation, including access-internal route installation
- DHCPv6 server groups
The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer’s edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the [edit system services dhcp-local-server] hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the [edit access address-assignment pool] hierarchy level using the family inet6 statement.

You can also include the dhcpv6 statement at the [edit routing-instances routing-instance-name system services dhcp-local-server] hierarchy.

NOTE: Existing DHCPv4 configurations in the [edit system services dhcp] hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 1007
Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 1010

Creating a Security Policy to Enable DHCPv6 Traffic

For the DHCPv6 server to allow DHCPv6 requests, you must create a security policy to enable DHCPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 2001:db8:3001::1.

To create a security zone policy to allow DHCPv6 on SRX1500, SRX5400, SRX5600, and SRX5800 devices:

1. Create the zone and add an interface to that zone.

   [edit security zones]
   user@host# edit security-zone my-zone interfaces ge-0/0/3.0

2. Configure host inbound traffic system services to allow DCHPv6.

   [edit security zones security-zone my-zone interfaces ge-0/0/3.0]
3. If you are done configuring the device, enter `commit` from configuration mode.

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 1007

**Example: Configuring DHCPv6 Server Options**

This example shows how to configure DHCPv6 server options on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

**Requirements**

Before you begin:

- Determine the IPv6 address pool range.
- Determine the IPv6 prefix. See the *Understanding Address Books*.
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients.
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.
Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the uptime command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 2001:db8:3001::1/64 and set router advertisement for interface ge-0/0/3.0. Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option dynamic-server to dynamically support prefix and attributes that are updated by the WAN server.

NOTE: A DHCPv6 group must contain at least one interface.

Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 uptime ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

   ```
   [edit]
   user@host# edit system services dhcp-local-server dhcpv6
   ```

2. Set a default limit for all DHCPv6 groups.
3. Specify a group name and interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0
```

4. Set a range of interfaces.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
```

5. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

6. Configure an interface with an IPv6 address.

```
[edit interfaces]
user@host# set ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
```

7. Set router advertisement for the interface.

```
[edit protocols]
user@host# set router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

**Results**

From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server`, `show interfaces ge-0/0/3`, and `show protocols` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.
[edit]
user@host# show interfaces ge-0/0/3
unit 0 {
family inet6 {
   address 2001:db8:3000::1/64;
}
}
[edit]
user@host# show protocols
router-advertisement {
   interface ge-0/0/3.0 {
      prefix 2001:db8:3000::1/64;
   }
}

If you are done configuring the device, enter commit from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying DHCPv6 Local Server Configuration

Purpose
Verify that the client address bindings and statistics for the DHCPv6 local server have been configured

Action
From operational mode, enter the show dhcpv6 server binding command to display the address bindings in the client table on the DHCPv6 local server.
From operational mode, enter the `show dhcv6 server statistics` command to display the DHCPv6 local server statistics.

```
Dhcpv6 Packets dropped:
   Total       0

Messages received:
   DHCPV6_DECLINE  0
   DHCPV6_SOLICIT  9
   DHCPV6_INFORMATION_REQUEST  0
   DHCPV6_RELEASE  0
   DHCPV6_REQUEST  5
   DHCPV6_CONFIRM  0
   DHCPV6_RENEW  0
   DHCPV6_REBIND  0
   DHCPV6_RELAY_FORW  0

Messages sent:
   DHCPV6_ADVERTISE  9
   DHCPV6_REPLY  5
   DHCPV6_RECONFIGURE  0
   DHCPV6_RELAY_REPL  0
```

- **clear dhcv6 server bindings all** command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance.

- **clear dhcv6 server statistics** command to clear all DHCPv6 local server statistics.
Understanding Cascaded DHCPv6 Prefix Delegating

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating device delegates IPv6 prefixes to a requesting device. The requesting device then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting device can also assign subnet addresses to subnets on the LAN.

With cascaded prefix delegation, the IPv6 address block is delegated to a DHCPv6 client that is running on the WAN interface of a customer edge device. The identity association (IA) for the client is used for the identity association for prefix delegation (IA_PD). The CE device requests, through DHCPv6, an IPv6 address with the IA type of nontemporary addresses (IA_NA). Both IA_PD and IA_NA are requesting in the same DHCPv6 exchange.

Figure 44: IPv6 Prefix Delegation

The topology in Figure 44 on page 969 shows an SRX Series device acting as the CPE. The WAN interface links to the provider edge (PE) device and the LAN interfaces link to the customer networks. The service provider delegates a prefix (delegated-prefix) and an IPv6 address (cpe-wan-ipv6-address) to a DHCPv6 client. When a requesting device receives that IPv6 address through the DHCPv6 client, the device must install the IPv6 address on its WAN interface. The DHCPv6 client then divides the delegated prefix into sub-prefixes and subsequently assigns them to the connected LAN interfaces of the CPE device, making some subset of the remaining space available for sub-prefix delegation.

A CPE assigns sub-prefixes to its LAN interfaces and broadcasts the sub-prefixes through device advertisement. In this scenario, the CPE acts as a sub-PE and delegates sub-prefixes and assigns them to sub-CPEs.
NOTE: The requirements of sub-prefix delegation are the same as for the prefix delegation defined in RFC 3769.

There can be multi-level sub prefix delegations, see Figure 45 on page 970. The top level CPE gets a delegated prefix from the PE and delegates the sub prefixes to second level sub-CPEs, then to the third level sub-CPEs, and finally to the end levels. The end level sub-CPEs assign the IPv6 address to end hosts through SLAAC, stateless DHCPv6 or stateful DHCPv6. This is called cascaded prefix delegating.

Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE)

This example shows how to configure DHCPv6 PD over PPPoE on SRX Series devices.
Requirements

No special configuration beyond the device initialization is required before configuring this feature.

Overview

The example uses SRX550M devices for configuring DHCPv6 PD over PPPoE. Before you begin, configure DHCPv6 server to permit in host-inbound traffic and receive DHCPv6 packet. Provide a host-name to establish PPPoE session. To enable IPv6, chassis reboot is required.

Configuring DHCPv6 PD over PPPoE involves the following configurations:

- Configuring DHCPv6 Server
- DHCPv6 Client (PD)
- DHCPv6 Client (Auto)

Topology

The following illustration describes DHCPv6 PD over PPPoE topology which provide a configuration suite using SRX Series devices.

Figure 46 on page 971 shows the topology used in this example.

Figure 46: Configuring SRX Series Devices for DHCPv6 PD over PPPoE

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

Quick configuration for DHCPv6 Server:

- DHCPv6 server configuration

```bash
set interfaces ge-0/0/2 unit 0 family inet6
```
• PPPoE configuration

set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap access-profile prof-ge001
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options server
set interfaces pp0 unit 0 family inet6 address 3000::1/64

• Router advertisement configuration

set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
set protocols router-advertisement interface pp0.0 managed-configuration
set protocols router-advertisement interface pp0.0 other-stateful-configuration
set protocols router-advertisement interface pp0.0 prefix 3000::1/64

• Enable IPv6

set security forwarding-options family inet6 mode flow-based

• PPPoE profile configuration

set access profile prof-ge001 client test_user chap-secret test

• PD address pool configuration

set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-length 48
set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-server 3000::1

• Security zone configuration

set security zones security-zone trust interface pp0.0 host-inbound-traffic system-services dhcpv6

Quick configuration for DHCPv6 Client (PD):

• DHCPv6 server configuration for autoconfig device
set interfaces ge-0/0/2 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0

- PPPoE configuration

set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
set interfaces pp0 unit 0 ppp-options chap local-name test_user
set interfaces pp0 unit 0 ppp-options chap passive
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options client

- DHCPv6 client configuration

set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0
  other-stateful-configuration
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0
  max-advertisement-interval 10
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0
  min-advertisement-interval 5
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
set protocols router-advertisement interface pp0.0

- Enable IPv6

set security forwarding-options family inet6 mode flow-based

- DHCPv6 server propagate configuration

set access address-assignment pool p1 family inet6 prefix 2001::/16
set access address-assignment pool p1 family inet6 dhcp-attributes propagate-settings pp0.0

- Security zone configuration

set security zones security-zone untrust interface pp0.0 host-inbound-traffic system-services dhcpv6
set security zones security-zone trust interface ge-0/0/2.0 host-inbound-traffic system-services dhcpv6
Quick configuration for DHCPv6 Client (Auto):

- DHCPv6 client configuration

  ```
  set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
  set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
  set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
  set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
  ```

- Router advertisement configuration

  ```
  set protocols router-advertisement interface fe-0/0/0.0
  ```

- Enable IPv6

  ```
  set security forwarding-options family inet6 mode flow-based
  ```

- Security zone configuration

  ```
  set security zones security-zone trust interface fe-0/0/0.0 host-inbound-traffic system-services dhcpv6
  ```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

1. To configure DHCPv6 server on SRX550M device:
   a. Set the interface.
   
   ```
   [edit]
   user@host# set interfaces ge-0/0/2 unit 0 family inet6
   ```
   b. Configure a DHCP local server.
   
   ```
   [edit]
   user@host# set system services dhcp-local-server dhcpv6
   ```
   c. Set a default limit for all DHCPv6 groups.
   
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set overrides interface-client-limit 100
   ```
   d. Set a custom client limit for the group.
   
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group overrides interface-client-limit 200
   ```
   e. Specify delegated pool name.
   
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group overrides delegated-pool v6-pd-pool
   ```
   f. Create a group called my-group that contains pp0 interface.
   
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set group my-group interface pp0.0
   ```

2. Configuring PPPoE:
   a. Set interface to encapsulate PPPoE.
   
   ```
   [edit]
   user@host# set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
   ```
   b. Set chap access profile value.
c. Set underlying interface name.

```bash
[edit system interface]
user@host# set interface pp0 unit 0 ppp-options chap access-profile prof-ge001
```

d. Set PPPoE-options server.

```bash
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

e. Set family name and address.

```bash
[edit system interface]
user@host# set interface pp0 unit 0 family inet6 address 3000::1/64
```

3. Configuring Router advertisement:

a. Set max advertisement interval limit.

```bash
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
```

b. Set minimum advertisement interval limit.

```bash
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
```

c. Set the configuration state to managed configuration.

```bash
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 managed-configuration
```

d. Set the configuration state to other stateful configuration.

```bash
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 other-stateful-configuration
```

e. Set the prefix value.
4. Enable IPv6:
   a. Set the family name and mode to enable IPv6.

   ```
   [edit]
   user@host# set protocols router-advertisement interface pp0.0 prefix 3000::1/64
   ```

5. Configuring PPPoE profile:
   a. Set access profile name, client name and chap secret.

   ```
   [edit]
   user@host# set access profile prof-ge001 client test user chap-secret test
   ```

6. Configuring PD address pool:
   a. Set address-assignment pool name, family name and prefix.

   ```
   [edit]
   user@host# set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
   ```
   b. Set range and prefix length.

   ```
   [edit]
   user@host# set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-length 48
   ```
   c. Set dhcp attributes with dns server value.

   ```
   [edit]
   user@host# set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-server 3000::1
   ```

7. Configuring Security zone:
   a. Set the zone name, interface and host-inbound-traffic system-services.

   ```
   [edit]
   user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic system-services dhcpv6
   ```

Step-by-Step Procedure
1. To configure DHCPv6 client (PD) on SRX550M device:
   a. Set the interface.
      
      ```
      [edit]
      user@host# set interfaces ge-0/0/2 unit 0 family inet6
      ```
   b. Set DHCPv6 local server to override the interface client limit.
      
      ```
      [edit]
      user@host# set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
      ```
   c. Set the process-inform pool name.
      
      ```
      [edit]
      user@host# set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
      ```
   d. Set group name and interface.
      
      ```
      [edit]
      user@host# set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
      ```

2. Configuring PPPoE:
   a. Set the interface to encapsulate ppp over ethernet.
      
      ```
      [edit system interface]
      user@host# set interface ge-0/0/1 unit 0 encapsulation ppp-over-ether
      ```
   b. Set default chap secret.
      
      ```
      [edit system interface]
      user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
      ```
   c. Set chap local name.
      
      ```
      [edit system interface]
      user@host# set interfaces pp0 unit 0 ppp-options chap local-name test_user
      ```
   d. Set PPP options chap state.
      
      ```
      [edit system interface]
      user@host# set interfaces pp0 unit 0 ppp-options chap passive
      ```
e. Set underlying-interface.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

f. Set pppoe-options.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options client
```

3. Configuring DHCPv6 client:

a. Set the family name and dhcpv6 client type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
```

b. Set the dhcpv6 client identity association type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
```

c. Set update-router-advertisement interface and other stateful-configuration.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0 other-stateful-configuration
```

d. Set maximum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0 max-advertisement-interval 10
```

e. Set minimum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface ge-0/0/2.0 min-advertisement-interval 5
```

f. Set client-identifier duid type.

```
[edit]
```
g. Set requested option for DHCPv6 client.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

h. Update the server.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
```

i. Set the protocols and the interface.

```
[edit]
user@host# set protocols router-advertisement interface pp0.0
```

4. Enable IPv6

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring DHCPv6 server to propagate DNS server information to end device:

a. Set address assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 prefix 2001::/16
```

b. Set the interface name for propagating TCP/IP settings to pool.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 dhcp-attributes propagate-settings pp0.0
```

6. Configuring security zone:

a. Set the zone name, untrust interface and system services.

```
[edit]
```
Step-by-Step Procedure

1. To configure DHCPv6 client (Auto) on SRX550M device:
   a. Set the interface, unit value, family name and DHCPv6 client type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
   ```
   b. Set Dhcpv6 client identity association type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
   ```
   c. Set client-identifier type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-11
   ```
   d. Set DHCPV6 client requested option.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
   ```

2. Configuring router advertisement:
   a. Set the protocol and interface.

   ```
   [edit]
   user@host# set protocols router-advertisement interface fe-0/0/0.0
   ```

   a. Set family name and mode.
4. Configuring security zone:

5. Set the zone name, trust interface and system services.

Results

- Result for DHCPv6 Server:

From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server`, `show interfaces`, `show protocols`, `show security forwarding-options`, `show access profile prof-ge001`, `show access address-assignment pool`, and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.
```plaintext
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}

pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
    }
}

ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}

pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}

pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
    }
}

...[edit]
user@host# show protocols
interface pp0.0 {
    max-advertisement-interval 20;
    min-advertisement-interval 10;
    managed-configuration;
    other-stateful-configuration;
    prefix 3000::1/64;
}
```
... [edit]
user@host# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
...
[edit]
user@host# show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
            ...
        }
    }
}
...
[edit]
user@host# show security zones
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
• Result for DHCPv6 Client (PD):

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
  overrides {
    interface-client-limit 10;
    process-inform {
      pool p1;
    }
  }
  group my-group {
    overrides {
      interface-client-limit 200;
      delegated-pool v6-pd-pool;
    }
    interface pp0.0;
  }
  group ipv6 {
    interface ge-0/0/2.0;
  }
}
...
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    encapsulation ppp-over-ether;
  }
}
pt-1/0/0 {
  vdsl-options {
    vdsl-profile auto;
  }
}
pp0 {
  unit 0 {
    ppp-options {
      chap {
        default-chap-secret "$ABC123"; ## SECRET-DATA
        local-name test_user;
      }
    }
  }
```
passive;
}

pppoe-options {
  underlying-interface ge-0/0/1.0;
  client;
}

family inet6 {
  dhcpv6-client {
    client-type statefull;
    client-ia-type ia-pd;
    update-router-advertisement {
      interface ge-0/0/2.0 {
        other-stateful-configuration;
        max-advertisement-interval 10;
        min-advertisement-interval 5;
      }
    }
    client-identifier duid-type duid-ll;
    req-option dns-server;
  }
}

[edit]
user@host# show interfaces pp0
unit 0 {
  ppp-options {
    chap {
      default-chap-secret "$ABC123"; ## SECRET-DATA
      local-name test_user;
      passive;
    }
  }
  pppoe-options {
    underlying-interface ge-0/0/1.0;
    client;
  }
}

[edit]
user@host# show security forwarding-options
family {
inet6 {
    mode flow-based;
}

...
[edit]
user@host# show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
        }
    }
}
pool p1 {
    family inet6 {
        prefix 2001::/16;
        dhcp-attributes {
            propagate-settings pp0.0;
        }
    }
}
...
[edit]
user@host# show access address-assignment
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {

dhcpv6;
}
}
}
ge-0/0/2.0 {
    host-inbound-traffic {
        system-services {
            dhcpv6;
        }
    }
}
}
}
}
}
security-zone untrust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}

• Result for DHCPv6 Client (Auto):

[edit]
user@host# show interfaces ge-0/0/0
unit 0 {
    family inet6 {
        dhcpv6-client {
            client-type autoconfig;
            client-ia-type ia-na;
            req-option dns-server;
        }
    }
}
...
[edit]
user@host# show protocols
router-advertisement {
    interface pp0.0 {
        max-advertisement-interval 20;
    }
}
min-advertisement-interval 10;
managed-configuration;
other-stateful-configuration;
prefix 3000::1/64;
}
interface fe-0/0/0.0;
}
...
[edit]
user@host# show security forwarding-options
family {
  inet6 {
    mode flow-based;
  }
}
...
[edit]
user@host# show security zones
security-zone Host {
  host-inbound-traffic {
    system-services{
      all;
    }
  }
  interfaces {
    ge-0/0/0.0;
  }
}
security-zone trust {
  interfaces {
    pp0.0 {
      host-inbound-traffic {
        system-services {
          dhcpv6;
        }
      }
    }
    ge-0/0/2.0 {
      host-inbound-traffic {
        system-services {
          dhcpv6;
        }
      }
    }
  }
}

Verification

Confirm that the configuration is working properly.

**Verifying DHCPv6 Server Configuration**

**Purpose**
Verify that the DHCPv6 Server has been configured.

**Action**
- From operational mode, enter the `show dhcpv6 server binding` command.

The following output shows the options for the `show dhcpv6 server binding` command.

```
[edit]
user@host> show dhcpv6 server binding detail
Session Id: 75
Client IPv6 Prefix: 2001:1:1::/48
Client DUID: LL0x1-3c:94:d5:98:90:01
State: BOUND (DHCPV6_LOCAL_SERVER_STATE_BOUND)
Lease Expires: 2016-03-26 10:12:37 JST
Lease Expires in: 86213 seconds
```
• From operational mode, enter the `show route table inet6.0` command.

The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:1:1::/48      *[Access/13] 00:03:45     <<<<<< Route for end device will be automatically generated
                     > to fe80::3e94:d50f:fc98:8600 via pp0.0
3000::/64          *[Direct/0] 00:04:04
                     > via pp0.0
3000::1/128        *[Local/0] 19:53:18
                     Local via pp0.0
fe80::b2c6:9a0f:fc7d:6900/128
                     *[Local/0] 19:53:18
                     Local via pp0.0
```

• From operational mode, enter the `show interfaces pp0.0 terse` command.

The following output shows the options for the `show interfaces pp0.0 terse` command.

```
[edit]
user@host>show interfaces pp0.0 terse
Interface       Admin Link Proto Local             Remote
pp0.0           up    up   inet6    3000::1/64
                           fe80::b2c6:9a0f:fc7d:6900/64
```

**Verifying DHCPv6 Client (PD) Configuration**

**Purpose**
Verify that the DHCPv6 Client (PD) has been configured.

**Action**
• From operational mode, enter the `show dhcpv6 client binding detail` command.
The following output shows the options for the `show dhcpv6 client binding detail` command.

```
[edit]
user@host>show dhcpv6 client binding detail

Client Interface: pp0.0  
   Hardware Address: 3c:94:d5:98:86:01  
   State: BOUND(DHCPV6_CLIENT_STATE_BOUND) <<<<< SRX is bound to prefix via pp0.0  

   ClientType: STATEFUL  
   Lease Expires: 2016-03-26 10:12:50 JST  
   Lease Expires in: 86232 seconds  
   Lease Start: 2016-03-25 10:12:50 JST  
   Bind Type: IA_PD  
   Client DUID: LL0x29-3c:94:d5:98:86:01  
   Rapid Commit: Off  
   Server Ip Address: fe80::b2c6:9a0f:fc7d:6900  
   Update Server: Yes  
   Client IP Prefix: 2001:1:1::/48

DHCP options:
   Name: server-identifier, Value: VENDOR0x00000583-0x41453530  
   Name: dns-recursive-server, Value: 3000::1
```

- From operational mode, enter the `show dhcpv6 server binding detail` command.

The following output shows the options for the `show dhcpv6 server binding detail` command.

```
[edit]
user@host>show dhcpv6 server binding detail

Session Id: 75  
   Client IPv6 Prefix: 2001:1:1::/48  
   Client DUID: LL0x1-3c:94:d5:98:90:01  
   State: BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)

   Lease Expires: 2016-03-26 10:12:37 JST  
   Lease Expires in: 86213 seconds  
   Lease Start: 2016-03-25 10:12:37 JST  
   Last Packet Received: 2016-03-25 10:12:50 JST  
   Incoming Client Interface: pp0.0  
   Server Ip Address: 0.0.0.0  
   Client Prefix Pool Name: v6-pd-pool  
   Client Id Length: 10  
   Client Id: /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the `show route table inet6.0` command.

The following output shows the options for the `show route table inet6.0` command.
From operational mode, enter the `show route table inet6.0` command.

The following output shows the options for the `show route table inet6.0` command.

| inet6.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden) |
|--------------------|-----------------|-----------------|
| + = Active Route, - = Last Active, * = Both |
| ::/0               | *[Access-internal/12] 00:03:35 |
|                    | > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0 |
| 2001:1:1::/64     | *[Direct/0] 00:03:48 |
|                    | > via ge-0/0/2.0 |
| 2001:1:1::1/128   | *[Local/0] 00:03:48 |
|                    | <<<<<< IPv6 address allocated by Prefix delegation |
|                    | Local via ge-0/0/2.0 |
| 3000::/64         | *[Access-internal/12] 00:03:35 |
|                    | > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0 |
| fe80::/64         | *[Direct/0] 00:03:48 |
|                    | > via ge-0/0/2.0 |
| fe80::3e94:d50f:fc98:8600/128 | *[Local/0] 19:05:19 |
|                    | Local via pp0.0 |
| fe80::3e94:d5ff:fe98:8602/128 | *[Local/0] 00:03:48 |
|                    | Local via ge-0/0/2.0 |

From operational mode, enter the `show interfaces pp0.0 terse` command.

The following output shows the options for the `show interfaces pp0.0 terse` command.

| [edit] |
| [edit] |
| `show interfaces pp0.0 terse` |
| user@host:~>show interfaces pp0.0 terse |
| Interface | Admin | Link | Proto | Local | Remote |
| pp0.0     | up    | up   | inet6 | fe80::3e94:d50f:fc98:8600/64 |

From operational mode, enter the `show interfaces ge-0/0/2.0 terse` command.

The following output shows the options for the `show interfaces ge-0/0/2.0 terse` command.

| [edit] |
| [edit] |
| `show interfaces ge-0/0/2.0 terse` |
| user@host:~>show interfaces ge-0/0/2.0 terse |
| Interface | Admin | Link | Proto | Local | Remote |
| ge-0/0/2.0 | up    | up   | inet6 | 2000:1:1::1/64 |
|            |       |      |       | fe80::3e94:d5ff:fe98:8602/64 |

From operational mode, enter the `show ipv6 router-advertisement` command.

The following output shows the options for the `show ipv6 router-advertisement` command.
Verifying DHCPv6 client (Auto) Configuration

Purpose
Verify that the DHCPv6 client (Auto) has been configured.

Action
• From operational mode, enter the show dhcpv6 client binding detail command.

The following output shows the options for the show dhcpv6 client binding detail command.
Rapid Commit: Off
Server Ip Address: fe80::3e94:d5ff:fe98:8602
Client IP Prefix: 2001:1:1::/64

DHCP options:
Name: server-identifier, Value: VENDOR0x00000583-0x414c3131

- From operational mode, enter the `show route table inet6.0` command.

The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
::/0  *[Access-internal/12] 00:02:36
    > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0/0.0
2001:1:1::/64   *[Access-internal/12] 00:02:36
    > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0/0.0
    *[Direct/0] 00:02:36
    > via fe-0/0/0/0.0
    [Local/0] 00:02:36
    Local via fe-0/0/0/0.0
fe80::/64  *[Direct/0] lw3d 15:51:19
    > via fe-0/0/0/0.0
fe80::226:88ff:fe38:b500/128
    *[Local/0] lw3d 15:51:19
    Local via fe-0/0/0/0.0
```

- From operational mode, enter the `show ipv6 router-advertisement` command.

The following output shows the options for the `show ipv6 router-advertisement` command.

```
[edit]
user@host>show ipv6 router-advertisement
Interface: fe-0/0/0/0.0
Advertisements sent: 1, last sent 00:02:45 ago
Solicits received: 0
Advertisements received: 8
Advertisement from fe80::3e94:d5ff:fe98:8602, heard 00:00:02 ago
    Managed: 0
    Other configuration: 1 [0]
```
Reachable time: 0 ms
Default lifetime: 30 sec [1800 sec]
Retransmit timer: 0 ms
Current hop limit: 64
Prefix: 2001:1:1:1::/64
  Valid lifetime: 86400 sec
  Preferred lifetime: 86400 sec
On link: 1
Autonomous: 1

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D70</td>
<td>Starting with Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, you can add the option dynamic-server to dynamically support prefix and attributes that are updated by the WAN server.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- DHCPv6 Client | 996
- Understanding DHCPv6 Client and Server Identification | 1005
- DHCPv6 Address-Assignment Pools | 1007

DHCPv6 Client

IN THIS SECTION

- DHCPv6 Client Overview | 998
- Minimum DHCPv6 Client Configuration | 998
- Configuring DHCP Client-Specific Attributes | 1000
- Configuring Optional DHCPv6 Client Attributes | 1001
- Configuring the DHCPv6 Client Rapid Commit Option | 1003
SRX Series device can act as a DHCPv6 client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. To enable a device to operate as a DHCPv6 client, you must configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. For more information, read this topic.
DHCPv6 Client Overview

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the `dhcpv6-client` statement at the `[edit interfaces]` hierarchy level.

NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the `[edit routing-instances]` hierarchy.

NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement
Minimum DHCPv6 Client Configuration

This topic describes the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
   ```

2. Configure the DHCPv6 client type. The client type can be autoconfig or statefull.
   - To enable DHCPv6 auto configuration mode, configure the client type as `autoconfig`.
     ```
     [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
     user@host# set client-type autoconfig
     ```
   - For stateful address assignment, configure the client type as `statefull`.
     ```
     [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
     user@host# set client-type statefull
     ```

3. Specify the identity association type.
   - To configure identity association for nontemporary address (IA_NA) assignment, specify the `client-ia-type` as `ia-na`.
     ```
     [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
     user@host# set client-ia-type ia-na
     ```
   - To configure identity association for prefix delegation (IA_PD), specify the `client-ia-type` as `ia-pd`.
     ```
     [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
     user@host# set client-ia-type ia-pd
     ```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:
   - Link Layer address (duid-ll)
   - Link Layer address plus time (duid-llt)
   - Vendor-assigned unique ID based on enterprise number (vendor)
NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [edit routing-instances] hierarchy.

### Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

NOTE: For SRX1500, SRX5400, SRX5600, and SRX5800 devices only.

You use the `dhcp-attributes` statement to configure DHCPv6 client-specific attributes for address-assignment pools at the [edit access address-assignment pool pool-name family inet6] hierarchy.

Table 60 on page 1000 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

#### Table 60: DHCPv6 Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>DHCPv6 Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns-server</td>
<td>IPv6 address of DNS server to which clients can send DNS queries</td>
<td>23</td>
</tr>
<tr>
<td>grace-period</td>
<td>Grace period offered with the lease</td>
<td>-</td>
</tr>
<tr>
<td>maximum-lease-time</td>
<td>Maximum lease time allowed by the DHCPv6 server</td>
<td>-</td>
</tr>
<tr>
<td>option</td>
<td>User-defined options</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 60: DHCPv6 Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>DHCPv6 Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip-server-address</td>
<td>IPv6 address of SIP outbound proxy server</td>
<td>22</td>
</tr>
<tr>
<td>sip-server-domain-name</td>
<td>Domain name of the SIP outbound proxy server</td>
<td>21</td>
</tr>
</tbody>
</table>

SEE ALSO

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 1010

Configuring Optional DHCPv6 Client Attributes

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:
   - dns-server
   - domain
   - ntp-server
   - sip-domain
   - sip-server

   For example, to specify the DHCPv6 client requested option as dns-server:

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set req-option dns-server
   ```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   ```
3. Configure the `update-server` option on the DHCPv6 client.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-server
   ```

4. Specify the interface used to delegate prefixes.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-router-advertisement interface ge-0/0/0
   ```

5. Configure the two-message (rapid commit) exchange option for address assignment.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set rapid-commit
   ```

**NOTE:** To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the `[edit routing-instances]` hierarchy.

**NOTE:** On all SRX Series devices, DHCPv6 client authentication is not supported.

**NOTE:** On SRX300, SRX320, SRX340, and SRX345, and SRX550M devices, DHCPv6 client does not support:
- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement
**Configuring the DHCPv6 Client Rapid Commit Option**

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```
Configuring a DHCPv6 Client in Autoconfig Mode

A DHCPv6 client configured in autoconfig mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in autoconfig mode on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as `autoconfig`.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-type autoconfig
   ```

2. Specify the identity association type as `ia-na` for nontemporary addresses.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-na
   ```

3. Specify the interface on which to configure router advertisement.

   ```
   [edit protocols router-advertisement]
   user@host# set interface ge-0/0/0
   ```
Configuring TCP/IP Propagation on a DHCPv6 Client

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the update-server option on the DHCPv6 client.

```plaintext
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

2. Configure the address pool to specify the interface (where update-server is configured) from which TCP/IP settings can be propagated.

```plaintext
[edit access]
user@host# set address-assignment pool 2 family inet6 dhcp-attributes propagate-settings ge-0/0/0
```

RELATED DOCUMENTATION

| DHCP Client | 933 |
| DHCPv6 Client | 996 |
| Understanding DHCPv6 Client and Server Identification | 1005 |

Understanding DHCPv6 Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or server. DHCPv6 clients use
DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-lit)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Layer address (duid-ll)

The duid-lit DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor’s registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

RELATED DOCUMENTATION

| DHCPv6 Client Overview | 998 |
DHCPv6 Address-Assignment Pools

IN THIS SECTION
- Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 1007
- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 1010
- Configuring an Address-Assignment Pool for Router Advertisement | 1011
- Configuring Nontemporary Address Assignment | 1012
- Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 1013
- Configuring Auto-Prefix Delegation | 1014

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address. For more information, read this topic.

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

IN THIS SECTION
- Requirements | 1008
- Overview | 1008
- Configuration | 1008
- Verification | 1010

This example shows how to configure an address-assignment pool on SRX1500, SRX5400, SRX5600, and SRX5800 devices.
Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool.
- Set DHCPv6 attributes for the address-assignment pool.

Overview

In this example, you configure an address-pool called my-pool and specify the IPv6 family as inet6. You configure the IPv6 prefix as 2001:db8:3000:1::/64, the range name as range1, and the IPv6 range for DHCPv6 clients from a low of 2001:db8:3000:1::/64 to a high of 2001:db8:3000:200::/64. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as 2001:db8:3001::1, the grace period as 3600, and the maximum lease time as 120.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

```plaintext
set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low 2001:db8:3000:1::/64 high 2001:db8:3000:200::/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server 2001:db8:3001::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period 3600
set access address-assignment pool my-pool family inet6 dhcp-attributes maximum-lease-time 120
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

   ```plaintext
   [edit access]
   user@host# edit address-assignment pool my-pool family inet6
   ```

2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.
3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:3001::1
```

4. Configure the DHCPv6 attribute for the grace period.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600
```

5. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes maximum-lease-time 120
```

**Results**

From configuration mode, confirm your configuration by entering the `show access address-assignment` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access address-assignment
pool my-pool {
family inet6 {
prefix 2001:db8:3000:1::/64;
range range1 {
  low 2001:db8:3000:1::/64;
  high 2001:db8:3000:200::/64;
}
dhcp-attributes {
  maximum-lease-time 120;
  grace-period 3600;
  dns-server {
    2001:db8:3001::1;
  }
}
```
If you are done configuring the device, enter **commit** from configuration mode.

**Verification**

Confirm that the configuration is working properly.

**Verifying Configuration**

**Purpose**
Verify that the address-assignment pool has been configured.

**Action**
From operational mode, enter the **show access address-assignment** command.

**SEE ALSO**

- DHCPv6 Server Overview | 962
- Example: Configuring DHCPv6 Server Options | 964
- Creating a Security Policy to Enable DHCPv6 Traffic | 963

### Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

**NOTE:** Supported only on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.
2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```plaintext
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 2001:db8:3000:5::/64
user@host# set range range2 low 2001:db8:3000:2::/64 high 2001:db8:3000:300::/64
```

3. Configure DHCPv6 attributes for the address pool.

```plaintext
[edit access address-assignment pool my-pool2 family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600 maximum-lease-time 120
```

4. If you are done configuring the device, enter `commit` from configuration mode.

SEE ALSO

| Configuring Address-Assignment Pool Linking | 932 |

### Configuring an Address-Assignment Pool for Router Advertisement

For SRX1500, SRX5400, SRX5600, and SRX5800 devices, you can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:


2. Specify that the address-assignment pool is used for router advertisement.

```plaintext
[edit access address-assignment]
```
user@host# set neighbor-discovery-router-advertisement router1

3. If you are done configuring the device, enter commit from configuration mode.

Configuring Nontemporary Address Assignment

Nontemporary address assignment is also known as stateful address assignment. In the stateful address assignment mode, the DHCPv6 client requests global addresses from the DHCPv6 server. Based on the DHCPv6 server’s response, the DHCPv6 client assigns the global addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client

2. Configure the client type as statefull.

   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-type statefull

3. Specify the IA_NA assignment.

   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-na

SEE ALSO

Minimum DHCPv6 Client Configuration | 998
**Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation**

The DHCPv6 client requests IPv6 addresses and prefixes from the DHCPv6 server. Based on the DHCPv6 server’s response, the DHCPv6 client assigns the IPv6 addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure identity association for nontemporary addresses (IA_NA) and identity association for prefix delegation (IA_PD) on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
   ```

2. Configure the client type as `statefull`.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-type statefull
   ```

3. Specify the IA_NA.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-na
   ```

4. Specify the IA_PD.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-pd
   ```

**SEE ALSO**

- Minimum DHCPv6 Client Configuration | 998
Configuring Auto-Prefix Delegation

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating router delegates IPv6 prefixes to a requesting router. The requesting router then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

To configure auto-prefix delegation for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as `statefull`.

   ```bash
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-type statefull
   ```

2. Specify the identity association type as `ia-na` for nontemporary addresses.

   ```bash
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-na
   ```

3. Specify the identity association type as `ia-pd` for prefix delegation.

   ```bash
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-ia-type ia-pd
   ```

4. Configure the DHCPv6 client identifier by specifying the DUID type.

   ```bash
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set client-identifier duid-type duid-ll
   ```

5. Specify the interface used to delegate prefixes.

   ```bash
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-router-advertisement interface ge-0/0/0
   ```

SEE ALSO

- Minimum DHCPv6 Client Configuration | 998
DHCP In Chassis Cluster Mode

Junos OS allows you to configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server and setup high availability between the two DHCP clients in chassis cluster mode.

Similarly, you can also configure two SRX Series devices as DHCP servers in chassis cluster mode and a third SRX Series device as a DHCP client. For more information, read this topic.

Example: Configuring the Device as a DHCP Server in Chassis Cluster Mode

IN THIS SECTION

- Requirements | 1016
- Overview | 1016
- Configuration | 1017
- Verification | 1022
This example shows how to configure a DHCP server in chassis cluster mode.

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP servers
- One SRX Series device as DHCP client
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP servers and a third SRX Series device as a DHCP client. Configure the two DHCP servers in chassis cluster mode.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface reth1.

For the DHCP client, you specify the interface as ge-0/0/1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.
WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices has been deprecated and only the new DHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

Configuration

CLI Quick Configuration
To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

Configure DHCP Server 1 and Server 2:

```
set system services dhcp-local-server group g1 interface reth1
set access address-assignment pool p1 family inet network 203.0.113.1/10
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Configure chassis cluster on DHCP Server 1 and DHCP Server 2:

```
set chassis cluster reth-count 4
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 2000
set chassis cluster redundancy-group 0 node 0 priority 200
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-6/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.1.1.1/24
```

Configure the DHCP client:

```
set interfaces ge-0/0/1 unit 0 family inet dhcp-client
```
Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure the devices as DHCP servers:

1. Configure the DHCP local server.

   ```
   [edit system services]
   user@host# set dhcp-local-server group g1 interface reth1
   ```

2. Configure an address pool.

   ```
   [edit access]
   user@host# set address-assignment pool p1 family inet network 203.0.113.1/10
   user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
   user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20
   ```

Step-by-Step Procedure
To configure the DHCP servers in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

   ```
   {primary:node0}[edit]
   user@host# set chassis cluster reth-count 4
   ```

2. Enable control link recovery.

   ```
   {primary:node0}[edit]
   user@host# set chassis cluster control-link-recovery
   ```

3. Configure heartbeat settings.
4. Configure the redundancy groups.

> {primary:node0}[edit]
> user@host# set chassis cluster heartbeat-interval 2000

> {primary:node0}[edit]
> user@host# set chassis cluster redundancy-group 0 node 0 priority 200
> user@host# set chassis cluster redundancy-group 0 node 1 priority 1

5. Configure redundant Ethernet interfaces.

> {primary:node0}[edit]
> user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
> user@host# set interfaces ge-6/0/1 gigether-options redundant-parent reth1
> user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
> user@host# set interfaces reth1 unit 0 family inet address 10.1.1.1/24

Step-by-Step Procedure
To configure the device as DHCP client:

1. Specify the DHCP client interface.

> [edit]
> user@host# edit interfaces ge-0/0/1 unit 0 family inet dhcp-client

2. Configure the DHCP client identifier as a hexadecimal value.

> [edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
> user@host# set client-identifier user-id ascii 00:0a:12:00:12:12

3. Set the DHCP lease time.

> [edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
> user@host# set lease-time 86400

4. Set the number of attempts allowed to retransmit a DHCP packet.

> [edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5

6. Set the IPv4 address of the preferred DHCP server.

[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1

7. Set the vendor class ID for the DHCP client.

[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether

Results
From configuration mode, confirm your configuration by entering the show commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show system services
dhcp-local-server {
    group g1 {
        interface reth1.0;
    }
}

[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
        network 203.0.113.1/10;
        range r1 {
            low 203.0.113.5;
            high 203.0.113.20;
        }
    }
}
[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 4;
heartbeat-interval 2000;
redundancy-group 0 {
    node 0 priority 200;
    node 1 priority 1;
}

[edit]
user@host# show interfaces reth1
redundant-ether-options {
    redundancy-group 1;
}
unit 0 {
    family inet {
        address 10.1.1.1.24;
    }
}

[edit]
user@host# show interfaces ge-0/0/1 unit 0 family inet
dhcp-client {
    client-identifier user-id ascii 00:0a:12:00:12:12;
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    server-address 10.1.1.1;
    vendor-id ether;
}

If you are done configuring the device, enter commit from configuration mode.
Verification

Verifying the DHCP Server in Chassis Cluster Mode

Purpose
Verify that the DHCP server is working in chassis cluster mode.

Action
From operational mode, enter the `show dhcp server binding` and `show dhcp server statistics` commands.

```
user@host> show dhcp server binding

<table>
<thead>
<tr>
<th>IP address</th>
<th>Session Id</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.1</td>
<td>1</td>
<td>64:87:88:79:a3:81</td>
<td>81855</td>
<td>BOUND</td>
<td>reth1</td>
</tr>
</tbody>
</table>

user@host> show dhcp server statistics

Packets dropped:
    Total                      0
    dhcp-service total         0

Messages received:
    BOOTREQUEST                2
    DHCPDECLINE                0
    DHCPDISCOVER               1
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                1

Messages sent:
    BOOTREPLY                  2
    DHCPOFFER                  1
    DHCPACK                    0
    DHCPNAK                    0
    DHCPFORCERENEW             0
```

Meaning
The sample output shows that DHCP servers configured in the example work in a chassis cluster.
This example shows how to configure the device as a DHCP client in chassis cluster mode.

**Requirements**

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP client
- One SRX Series device as DHCP server
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.
- Determine the DHCP options required by the subnets and clients in your network.

**Overview**

In this example, you configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server. Configure the two DHCP clients in chassis cluster mode.
For DHCP clients, you specify the interface as reth1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time with the packets. You set the DHCP lease name as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds. You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 203.0.113.1 and the vendor class ID to ether.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface ge-0/0/2.0.

**Configuration**

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter commit from configuration mode.

Configure DHCP Client 1 and Client 2:

```
set interfaces reth1 unit 0 family inet dhcp-client
set interfaces reth1 unit 0 family inet dhcp-client client-identifier user-id ascii 00:0a:12:00:12:12
set interfaces reth1 unit 0 family inet dhcp-client options no-hostname
set interfaces reth1 unit 0 family inet dhcp-client lease-time 86400
set interfaces reth1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces reth1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces reth1 unit 0 family inet dhcp-client server-address 203.0.113.1
set interfaces reth1 unit 0 family inet dhcp-client vendor-id ether
```

Configure chassis cluster on Client 1 and Client 2:

```
set chassis cluster reth-count 2
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 1000
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-4/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
```
Configure the DHCP server:

```
set system service dhcp-local-server group g1 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
set access address-assignment pool p1 family inet network 203.0.113.0/24
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the devices as DHCP clients:

1. Specify the DHCP client interface.

   ```
   [edit]
   user@host# edit interfaces reth1 unit 0 family inet dhcp-client
   ```

2. Configure the DHCP client identifier as a hexadecimal value.

   ```
   [edit interfaces reth1 unit 0 family inet dhcp-client]
   user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
   ```

3. Set the hostname if you do not want the DHCP client to send hostname in the packets (RFC option code 12).

   ```
   [edit interfaces reth1 unit 0 family inet dhcp-client]
   user@host# set options no-hostname
   ```

4. Set the DHCP lease time.

   ```
   [edit interfaces reth1 unit 0 family inet dhcp-client]
   user@host# set lease-time 86400
   ```

5. Set the number of attempts allowed to retransmit a DHCP packet.

   ```
   [edit interfaces reth1 unit 0 family inet dhcp-client]
   user@host# set retransmission-attempt 6
   ```
6. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5

7. Set the IPv4 address of the preferred DHCP server.

[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set server-address 203.0.113.1

8. Set the vendor class ID for the DHCP client.

[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether

Step-by-Step Procedure
To configure the DHCP clients in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

{primary:node0}[edit]
user@host# set chassis cluster reth-count 2

2. Enable control link recovery.

{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery

3. Configure heartbeat settings.

{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 1000

4. Configure the redundancy groups.

{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 node 0 priority 100
user@host# set chassis cluster redundancy-group 1 node 1 priority 1
user@host# set chassis cluster redundancy-group 0 node 0 priority 100
user@host# set chassis cluster redundancy-group 0 node 1 priority 1

5. Configure redundant Ethernet interfaces.

{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1

Step-by-Step Procedure
To configure the device as DHCP server:

1. Configure the DHCP local server.

[edit system services]
user@host# set dhcp-local-server group g1 interface ge-0/0/2

2. Configure IP address of the server.

[edit interfaces]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24

3. Configure an address pool.

[edit access]
user@host# set address-assignment pool p1 family inet network 203.0.113.0/24
user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20

Results
From configuration mode, confirm your configuration by entering the show commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show interfaces reth1 unit 0 family inet
dhcp-client {
    client-identifier user-id ascii 00:0a:12:00:12:12;
options no-hostname;
lease-time 86400;
retransmission-attempt 6;
retransmission-interval 5;
server-address 203.0.113.1;
vendor-id ether;

[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 2;
heartbeat-interval 1000;
redundancy-group 0 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 1{
    node 0 priority 100;
    node 1 priority 1;
}

[edit]
user@host# show interfaces reth1
redundant-ether-options {
    redundancy-group 1;
}

[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
        network 203.0.113.0/24;
        range r1 {
            low 203.0.113.5;
            high 203.0.113.20;
        }
    }
}

If you are done configuring the device, enter commit from configuration mode.
Verification

Confirm that the configuration is working properly.

*Verifying the DHCP Client in Chassis Cluster Mode*

**Purpose**
Verify that the DHCP client is working in chassis cluster mode.

**Action**
From operational mode, enter the `show dhcp client binding`, `show dhcp client statistics` and `show dhcp client binding interface reth1 detail` commands.

```
user@host> show dhcp client binding

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.0.113.14</td>
<td>00:1f:12:e3:34:01</td>
<td>84587</td>
<td>BOUND</td>
<td>reth1.0</td>
</tr>
</tbody>
</table>

user@host> show dhcp client statistics

Packets dropped:
  Total 4
  Send error 4

Messages received:
  BOOTREPLY 3
  DHCPoffer 1
  DHCPack 2
  DHCPnak 0
  DHCPforcerenew 0

Messages sent:
  BOOTREQUEST 0
  DHCPdecline 0
  DHCPdiscover 5
  DHCPrequest 8
  DHCPinform 0
  DHCPrelease 1
  DHCPrenew 0
  DHCPrebind 0
```
show dhcp client binding interface reth1 detail

Client Interface: reth1.0
Hardware Address: 00:10:db:ff:10:01
State: BOUND (LOCAL_CLIENT_STATE_BOUND)
Lease Expires: 2013-12-18 10:15:36 CST
Lease Expires in: 30 seconds
Lease Start: 2013-12-17 10:15:36 CST
Server Identifier: 203.0.113.1
Client IP Address: 10.1.1.14
Update Server: No

DHCP options:
  Name: dhcp-lease-time, Value: 1 day
  Name: server-identifier, Value: 10.1.1.1
  Name: subnet-mask, Value: 255.255.255.0

Meaning
The sample output shows that DHCP clients configured in the example work in a chassis cluster.

SEE ALSO
- Understanding DHCP Client Operation | 933

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1X49-D60</td>
<td>Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices has been deprecated and only the new DHCP CLI is supported.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

- Configuring Chassis Clustering on an SRX Series Devices
- DHCP Overview | 909
- DHCP Server | 915
Permission Flags

access | 1035
access-control | 1040
admin | 1041
admin-control | 1047
all-control | 1048
clear | 1049
configure | 1150
control | 1151
field | 1152
firewall | 1153
firewall-control | 1159
floppy | 1160
flow-tap | 1161
flow-tap-control | 1165
flow-tap-operation | 1166
idp-profiler-operation | 1167
interface | 1168
interface-control | 1173
maintenance | 1175
network | 1187
pgcp-session-mirroring | 1190
pgcp-session-mirroring-control | 1195
reset | 1196
rollback | 1197
routing | 1198
routing-control | 1209
secret | 1215
secret-control | 1221
security | 1223
security-control | 1233
shell | 1238
snmp | 1239
snmp-control | 1243
system | 1244
system-control | 1252
trace | 1255
trace-control | 1266
view | 1274
view-configuration | 1423
Can view the access configuration in configuration mode.

**Commands**

- `clear unified-edge`
- `clear unified-edge ggsn-pgw`
- `clear unified-edge ggsn-pgw aaa`
- `clear unified-edge ggsn-pgw aaa radius`
- `clear unified-edge ggsn-pgw aaa radius statistics`
- `clear unified-edge ggsn-pgw aaa statistics`
- `clear unified-edge ggsn-pgw address-assignment`
- `clear unified-edge ggsn-pgw address-assignment pool`
- `clear unified-edge ggsn-pgw address-assignment statistics`
- `clear unified-edge ggsn-pgw call-admission-control`
- `clear unified-edge ggsn-pgw call-admission-control statistics`
- `clear unified-edge ggsn-pgw charging`
- `clear unified-edge ggsn-pgw charging cdr`
- `clear unified-edge ggsn-pgw charging cdr wfa`
- `clear unified-edge ggsn-pgw charging local-persistent-storage`
- `clear unified-edge ggsn-pgw charging local-persistent-storage statistics`
- `clear unified-edge ggsn-pgw charging path`
- `clear unified-edge ggsn-pgw charging path statistics`
- `clear unified-edge ggsn-pgw charging transfer`
- `clear unified-edge ggsn-pgw charging transfer statistics`
- `clear unified-edge ggsn-pgw diameter`
- `clear unified-edge ggsn-pgw diameter dcca-gy`
- `clear unified-edge ggsn-pgw diameter dcca-gy statistics`
- `clear unified-edge ggsn-pgw diameter network-element`
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp peer
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw ip-reassembly
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
<clear-mobile-gateway-sgw-call-admission-control>
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
Configuration Hierarchy Levels

[edit access]
[edit access diameter]
[edit access ppp-options]
[edit access radius]
[edit dynamic-profile]
[edit logical-systems access]
[edit logical-systems routing-instances instance system services static-subscribers access-profile]
[edit logical-systems routing-instances instance system services static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers access-profile]
[edit routing-instances instance system services static-subscribers dynamic-profile]
[edit routing-instances instance system services static-subscribers group access-profile]
[edit routing-instances instance system services static-subscribers group dynamic-profile]
access-control

Can view access configuration information. Can edit access configuration at the [edit access], [edit logical-systems], [edit routing-instances], and [edit system services] hierarchy levels.

Configuration Hierarchy Levels
static-subscribers dynamic-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group access-profile]
[edit logical-systems routing-instances instance system services
static-subscribers group dynamic-profile]
[edit logical-systems system services static-subscribers access-profile]
[edit logical-systems system services static-subscribers dynamic-profile]
[edit logical-systems system services static-subscribers group access-profile]
[edit logical-systems system services static-subscribers group dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
dynamic-profile]
[edit routing-instances instance system services static-subscribers
access-profile]
[edit routing-instances instance system services static-subscribers
group access-profile]
[edit routing-instances instance system services static-subscribers
group dynamic-profile]
[edit system services static-subscribers access-profile]
[edit system services static-subscribers dynamic-profile]
[edit system services static-subscribers group access-profile]
[edit system services static-subscribers group dynamic-profile]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
access | 1035

Can view user account information in configuration mode.
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dccagx
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
task unified-edge ggsn-pgw
task unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
task unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
task unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
task unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
task unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
task unified-edge sgw
task unified-edge sgw call-trace
task unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
task unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
task unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
task unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
task unified-edge tdf
request unified-edge tdf call-trace
task unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
task unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show system audit

Configuration Hierarchy Levels

[edit protocols uplink-failure-detection]
[edit system]
[edit system accounting]
[edit system diag-port-authentication]
[edit system extensions]
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh authorized-keys-command]
[edit system services ssh authorized-keys-command-user]
[edit system services ssh ciphers]
[edit system services ssh client-alive-count-max]
[edit system services ssh client-alive-interval]]
[edit system services ssh fingerprint-hash]
[edit system services ssh hostkey-algorithm]
[edit system services ssh key-exchange]
[edit system services ssh macs]
[edit system services ssh max-sessions-per-connection]
[edit system services ssh no-tcp-forwarding]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
[edit system services ssh tcp-forwarding]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
admin-control

Can view user account information and configure it at the [edit system] hierarchy level.

Commands

```plaintext
show system audit
```

Configuration Hierarchy Levels

```plaintext
[edit protocols uplink-failure-detection]
[edit system]
[edit system accounting]
[edit system diag-port-authentication]
[edit system extensions]
[edit system login]
[edit system pic-console-authentication]
[edit system root-authentication]
[edit system services ssh ciphers]
[edit system services ssh hostkey-algorithm]
[edit system services ssh key-exchange]
[edit system services ssh macs]
[edit system services ssh protocol-version]
[edit system services ssh root-login]
```
all-control

Can access all operational mode commands and configuration mode commands. Can modify configuration in all the configuration hierarchy levels.

Commands

All CLI commands.

Configuration Hierarchy Levels

All CLI configuration hierarchy levels and statements.
clear

Can clear (delete) information learned from the network that is stored in various network databases.

Commands

```
clear
clear access-security
clear access-security router-advertisement-entries
<clear-as-router-advertisement-entry>
clear amt
clear amt statistics
<clear-amt-statistics>
clear amt tunnel
clear-amt-tunnel
clear amt tunnel gateway-address
<clear amt tunnel gateway-address>
clear amt tunnel statistics
<clear-amt-tunnel-statistics>
clear amt tunnel statistics gateway-address
<clear-amt-tunnel-gateway-address-statistics>
clear amt tunnel statistics tunnel-interface
<clear-amt-tunnel-interface-statistics>
clear amt tunnel tunnel-interface
<clear-amt-tunnel-interface>
clear ancp
clear ancp neighbor
<clear-ancp-neighbor-connection>
clear ancp statistics
<clear-ancp-statistics>
clear ancp subscriber
<clear-ancp-subscriber-connection>
clear-appqos-counter
<clear-appqos-rate-limiters-statistics>
clear-appqos-rate-limiter-statistics
clear-appqos-rule-statistics
clear arp
<clear-arp-table>
clear auto-configuration
clear auto-configuration interfaces
<clear-auto-configuration-interfaces>
```
clear bfd
clear bfd adaptation
<clear-bfd-adaptation-information>
clear bfd adaptation address
<clear-bfd-adaptation-address>
clear bfd adaptation discriminator
<clear-bfd-adaptation-discriminator>
clear bfd session
<clear-bfd-session-information>
clear bfd session address
<clear-bfd-session-address>
clear bfd session discriminator
<clear-bfd-session-discriminator>
clear bgp
clear bgp damping
<clear-bgp-damping>
clear bgp neighbor
<clear-bgp-neighbor>
clear bgp table
<clear-bgp-table>
clear bridge
clear bridge evpn
clear bridge evpn arp-table
<clear-bridge-evpn-arp-table>
clear bridge evpn nd-table
<clear-bridge-evpn-nd-table>
clear bridge mac-table
<clear-bridge-mac-table>
clear bridge mac-table interface
<clear-bridge-interface-mac-table>
clear bridge recovery-timeout
<clear-bridge-recovery>
clear bridge recovery-timeout interface
<clear-bridge-recovery-interface>
clear bridge satellite
clear bridge satellite logging
<clear-satellite-control-logging>
clear bridge satellite vlan-auto-sense
<clear-satellite-control-plane-vlan-auto-sense>
clear captive-portal
clear captive-portal firewall
<clear-captive-portal-firewall>
clear captive-portal firewall interface
<clear-captive-portal-firewall-interface>
clear captive-portal interface
<clear-captive-portal-interface-session>
clear captive-portal mac-address
<clear-captive-portal-mac-session>
clear cli
clear cli logical-system
<clear-cli-logical-system>
clear database-replication
clear database-replication statistics
<clear-database-replication-statistics-information>
clear ddos-protection
clear ddos-protection protocols
clear ddos-protection protocols all-fiber-channel-enode
clear ddos-protection protocols all-fiber-channel-enode aggregate
clear ddos-protection protocols all-fiber-channel-enode aggregate culprit-flows
<clear-ddos-all-fc-enode-aggregate-flows>
clear ddos-protection protocols all-fiber-channel-enode aggregate states
<clear-ddos-all-fc-enode-aggregate-states>
clear ddos-protection protocols all-fiber-channel-enode aggregate statistics
<clear-ddos-all-fc-enode-aggregate-statistics>
clear ddos-protection protocols all-fiber-channel-enode culprit-flows
<clear-ddos-all-fc-enode-flows>
clear ddos-protection protocols all-fiber-channel-enode states
<clear-ddos-all-fc-enode-states>
clear ddos-protection protocols all-fiber-channel-enode statistics
<clear-ddos-all-fc-enode-statistics>
clear ddos-protection protocols amtv4
clear ddos-protection protocols amtv4 aggregate
clear ddos-protection protocols amtv4 aggregate culprit-flows
<clear-ddos-amtv4-aggregate-flows>
clear ddos-protection protocols amtv4 aggregate states
<clear-ddos-amtv4-aggregate-states>
clear ddos-protection protocols amtv4 aggregate statistics
<clear-ddos-amtv4-aggregate-statistics>
clear ddos-protection protocols amtv4 culprit-flows
<clear-ddos-amtv4-culprit-flows>
clear ddos-protection protocols amtv4 states
<clear-ddos-amtv4-states>
clear ddos-protection protocols amtv4 statistics
<clear-ddos-amtv4-statistics>
clear ddos-protection protocols amtv6
clear ddos-protection protocols amtv6 aggregate
clear ddos-protection protocols amtv6 aggregate culprit-flows
<clear-ddos-amtv6-aggregate-flows>
clear ddos-protection protocols amtv6 aggregate states
<clear-ddos-amtv6-aggregate-states>
clear ddos-protection protocols amtv6 aggregate statistics
<clear-ddos-amtv6-aggregate-statistics>
clear ddos-protection protocols amtv6 culprit-flows
<clear-ddos-amtv6-flows>
clear ddos-protection protocols amtv6 states
<clear-ddos-amtv6-states>
clear ddos-protection protocols amtv6 statistics
<clear-ddos-amtv6-statistics>
clear ddos-protection protocols ancp aggregate culprit-flows
<clear-ddos-ancp-aggregate-flows>
clear ddos-protection protocols ancp culprit-flows
<clear-ddos-ancp-flows>
clear ddos-protection protocols ancp aggregate
<clear-ddos-ancp-aggregate>
clear ddos-protection protocols ancp aggregate states
<clear-ddos-ancp-aggregate-states>
clear ddos-protection protocols ancp aggregate statistics
<clear-ddos-ancp-aggregate-statistics>
clear ddos-protection protocols ancp states
<clear-ddos-ancp-states>
clear ddos-protection protocols ancp statistics
<clear-ddos-ancp-statistics>
clear ddos-protection protocols ancpv6 aggregate
<clear-ddos-ancpv6-aggregate>
clear ddos-protection protocols ancpv6 aggregate culprit-flows
<clear-ddos-ancpv6-aggregate-flows>
clear ddos-protection protocols ancpv6 aggregate states
<clear-ddos-ancpv6-aggregate-states>
clear ddos-protection protocols ancpv6 aggregate statistics
<clear-ddos-ancpv6-aggregate-statistics>
clear ddos-protection protocols arp aggregate culprit-flows
<clear-ddos-arp-aggregate-flows>
clear ddos-protection protocols arp aggregate states
<clear-ddos-arp-aggregate-states>
clear ddos-protection protocols arp aggregate statistics
<clear-ddos-arp-aggregate-statistics>
clear ddos-protection protocols arp states
<clear-ddos-arp-states>
clear ddos-protection protocols arp statistics
<clear-ddos-arp-statistics>
clear ddos-protection protocols arp-snoop aggregate
<clear-ddos-arp-snoop-aggregate>
clear ddos-protection protocols arp-snoop aggregate culprit-flows
<clear-ddos-arp-snoop-aggregate-flows>
clear ddos-protection protocols arp-snoop aggregate states
<clear-ddos-arp-snoop-aggregate-states>
clear ddos-protection protocols arp-snoop aggregate statistics
<clear-ddos-arp-snoop-aggregate-statistics>
clear ddos-protection protocols arp-snoop culprit-flows
<clear-ddos-arp-snoop-flows>
clear ddos-protection protocols arp-snoop states
<clear-ddos-arp-snoop-states>
clear ddos-protection protocols arp-snoop statistics
<clear-ddos-arp-snoop-statistics>
clear ddos-protection protocols atm
clear ddos-protection protocols atm aggregate
clear ddos-protection protocols atm aggregate culprit-flows
<clear-ddos-atm-aggregate-states>
clear ddos-protection protocols atm aggregate statistics
<clear-ddos-atm-aggregate-statistics>
clear ddos-protection protocols atm culprit-flows
clear ddos-protection protocols atm states
clear-ddos-atm-states
clear ddos-protection protocols atm statistics
clear-ddos-atm-statistics
clear ddos-protection protocols bfd
clear ddos-protection protocols bfd aggregate
clear ddos-protection protocols bfd culprit-flows
clear ddos-protection protocols bfd aggregate states
clear-ddos-bfd-aggregate-states
clear ddos-protection protocols bfd aggregate statistics
<clear-ddos-bfd-aggregate-statistics>
clear ddos-protection protocols bfd states
<clear-ddos-bfd-states>
clear ddos-protection protocols bfd statistics
<clear-ddos-bfd-statistics>
clear ddos-protection protocols bfdv6
clear ddos-protection protocols bfdv6 aggregate
clear ddos-protection protocols bfdv6 culprit-flows
clear ddos-protection protocols bfdv6 aggregate states
<clear-ddos-bfdv6-aggregate-states>
clear ddos-protection protocols bfdv6 aggregate statistics
<clear-ddos-bfdv6-aggregate-statistics>
clear ddos-protection protocols bfdv6 states
<clear-ddos-bfdv6-states>
clear ddos-protection protocols bfdv6 statistics
<clear-ddos-bfdv6-statistics>
clear ddos-protection protocols bgp
clear ddos-protection protocols bgp aggregate
clear ddos-protection protocols bgp aggregate culprit-flows
clear ddos-protection protocols bgp aggregate states
clear-ddos-bgp-aggregate-states
clear ddos-protection protocols bgp aggregate statistics
clear ddos-protection protocols bgp culprit-flows
clear ddos-protection protocols bgp states
clear-ddos-bgp-states
clear ddos-protection protocols bgp statistics
clear-ddos-bgp-statistics
clear ddos-protection protocols bgpv6
clear ddos-protection protocols bgpv6 aggregate
clear ddos-protection protocols bgpv6 aggregate culprit-flows
clear ddos-protection protocols bgpv6 aggregate states
clear-ddos-bgpv6-aggregate-states
clear ddos-protection protocols bgpv6 aggregate statistics
clear-ddos-bgpv6-aggregate-statistics
clear ddos-protection protocols bgpv6 states
clear-ddos-bgpv6-states
clear ddos-protection protocols bgpv6 aggregate statistics
<clear-ddos-bgpv6-statistics>
clear ddos-protection protocols bridge-control
clear ddos-protection protocols bridge-control aggregate
clear ddos-protection protocols bridge-control aggregate culprit-flows
<clear-ddos-brg-ctrl-aggregate-flows>
clear ddos-protection protocols bridge-control aggregate states
<clear-ddos-brg-ctrl-aggregate-states>
clear ddos-protection protocols bridge-control aggregate statistics
<clear-ddos-brg-ctrl-aggregate-statistics>
clear ddos-protection protocols bridge-control culprit-flows
<clear-ddos-brg-ctrl-flows>
clear ddos-protection protocols bridge-control states
<clear-ddos-brg-ctrl-states>
clear ddos-protection protocols bridge-control statistics
<clear-ddos-brg-ctrl-statistics>
clear ddos-protection protocols culprit-flows
clear ddos-protection protocols demux-autosense
clear ddos-protection protocols demux-autosense aggregate
clear ddos-protection protocols demux-autosense aggregate culprit-flows
clear ddos-protection protocols demux-autosense aggregate states
clear-ddos-demuxauto-aggregate-states
clear ddos-protection protocols demux-autosense aggregate statistics
clear ddos-protection protocols demux-autosense culprit-flows
clear ddos-protection protocols demux-autosense states
clear-ddos-demuxauto-states
clear ddos-protection protocols demux-autosense statistics
clear-ddos-demuxauto-statistics
clear ddos-protection protocols dhcpv4
clear ddos-protection protocols dhcpv4 ack
clear ddos-protection protocols dhcpv4 ack culprit-flows
clear ddos-protection protocols dhcpv4 ack states
clear ddos-protection protocols dhcpv4 ack statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4v6
clear ddos-protection protocols dhcpv4v6 aggregate
clear ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<clear-ddos-dhcpv4v6-aggregate-flows>
clear ddos-protection protocols dhcpv4v6 aggregate states
<clear-ddos-dhcpv4v6-aggregate-states>
clear ddos-protection protocols dhcpv4v6 aggregate statistics
<clear-ddos-dhcpv4v6-aggregate-statistics>
clear ddos-protection protocols dhcpv4v6 culprit-flows
<clear-ddos-dhcpv4v6-flows>
clear ddos-protection protocols dhcpv4v6 states
<clear-ddos-dhcpv4v6-states>
clear ddos-protection protocols dhcpv4v6 statistics
<clear-ddos-dhcpv4v6-statistics>
clear-ddos-demuxauto-aggregate-states
clear-ddos-demuxauto-aggregate-statistics
clear-ddos-demuxauto-states
clear-ddos-demuxauto-statistics
clear-ddos-dhcpv4-ack-states
clear ddos-protection protocols dhcpv4 ack statistics
clear-ddos-dhcpv4-ack-statistics
clear ddos-protection protocols dhcpv4 aggregate
clear ddos-protection protocols dhcpv4 aggregate states
clear-ddos-dhcpv4-aggregate-states
clear ddos-protection protocols dhcpv4 aggregate statistics
clear-ddos-dhcpv4-aggregate-statistics
clear ddos-protection protocols dhcpv4 bad-packets
clear ddos-protection protocols dhcpv4 bad-packets states
clear-ddos-dhcpv4-bad-pack-states
clear ddos-protection protocols dhcpv4 bad-packets statistics
clear-ddos-dhcpv4-bad-pack-statistics
clear ddos-protection protocols dhcpv4 bootp
clear ddos-protection protocols dhcpv4 bootp states
clear-ddos-dhcpv4-bootp-states
clear ddos-protection protocols dhcpv4 bootp statistics
clear-ddos-dhcpv4-bootp-statistics
clear ddos-protection protocols dhcpv4 decline
clear ddos-protection protocols dhcpv4 decline culprit-flows
clear ddos-protection protocols dhcpv4 decline states
clear-ddos-dhcpv4-decline-states
clear ddos-protection protocols dhcpv4 decline statistics
clear-ddos-dhcpv4-decline-statistics
clear ddos-protection protocols dhcpv4 discover
clear ddos-protection protocols dhcpv4 discover states
clear-ddos-dhcpv4-discover-states
clear ddos-protection protocols dhcpv4 discover statistics
clear-ddos-dhcpv4-discover-statistics
clear ddos-protection protocols dhcpv4 force-renew
clear ddos-protection protocols dhcpv4 force-renew culprit-flows
clear ddos-protection protocols dhcpv4 force-renew states
clear-ddos-dhcpv4-force-renew-states
clear ddos-protection protocols dhcpv4 force-renew statistics
clear-ddos-dhcpv4-force-renew-statistics
clear ddos-protection protocols dhcpv4 inform
clear ddos-protection protocols dhcpv4 inform culprit-flows
clear ddos-protection protocols dhcpv4 inform states
clear-ddos-dhcpv4-inform-states
clear ddos-protection protocols dhcpv4 inform statistics
clear-ddos-dhcpv4-inform-statistics
clear ddos-protection protocols dhcpv4 unclassified culprit-flows
clear ddos-protection protocols dhcpv4 unclassified states
clear-ddos-dhcpv4-unclass-states
clear ddos-protection protocols dhcpv4 unclassified statistics
clear-ddos-dhcpv4-unclass-statistics
clear ddos-protection protocols dhcpv6
clear ddos-protection protocols dhcpv6 advertise
clear ddos-protection protocols dhcpv6 advertise culprit-flows
clear ddos-protection protocols dhcpv6 advertise states
clear-ddos-dhcpv6-advertise-states
clear ddos-protection protocols dhcpv6 advertise statistics
clear-ddos-dhcpv6-advertise-statistics
clear ddos-protection protocols dhcpv6 aggregate
clear-ddos-dhcpv6-aggregate
clear ddos-protection protocols dhcpv6 aggregate states
clear-ddos-dhcpv6-aggregate-states
clear ddos-protection protocols dhcpv6 aggregate statistics
clear-ddos-dhcpv6-aggregate-statistics
clear ddos-protection protocols dhcpv6 confirm
clear ddos-protection protocols dhcpv6 confirm culprit-flows
clear ddos-protection protocols dhcpv6 confirm states
clear-ddos-dhcpv6-confirm-states
clear ddos-protection protocols dhcpv6 confirm statistics
clear-ddos-dhcpv6-confirm-statistics
clear ddos-protection protocols dhcpv6 decline
clear ddos-protection protocols dhcpv6 decline states
clear-ddos-dhcpv6-decline-states
clear ddos-protection protocols dhcpv6 decline statistics
clear-ddos-dhcpv6-decline-statistics
clear ddos-protection protocols dhcpv6 information-request
clear ddos-protection protocols dhcpv6 information-request states
clear-ddos-dhcpv6-info-req-states
clear ddos-protection protocols dhcpv6 information-request statistics
clear-ddos-dhcpv6-info-req-statistics
clear ddos-protection protocols dhcpv6 leasequery
clear ddos-protection protocols dhcpv6 leasequery states
clear-ddos-dhcpv6-leasequery-states
clear ddos-protection protocols dhcpv6 leasequery statistics
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-data
clear ddos-protection protocols dhcpv6 leasequery-data states
clear ddos-protection protocols dhcpv6 leasequery-data statistics
clear ddos-protection protocols garp-reply
clear ddos-protection protocols garp-reply aggregate
clear ddos-protection protocols garp-reply aggregate culprit-flows
<clear-ddos-garp-reply-aggregate-flows>
clear ddos-protection protocols garp-reply aggregate states
<clear-ddos-garp-reply-aggregate-states>
clear ddos-protection protocols garp-reply aggregate statistics
<clear-ddos-garp-reply-aggregate-statistics>
clear ddos-protection protocols garp-reply culprit-flows
<clear-ddos-garp-reply-flows>
clear ddos-protection protocols garp-reply states
<clear-ddos-garp-reply-states>
clear ddos-protection protocols garp-reply statistics
<clear-ddos-garp-reply-statistics>
clear ddos-protection protocols gre hbc
<clear-ddos-gre-hbc-flows>
clear ddos-protection protocols gre hbc states
<clear-ddos-gre-hbc-states>
clear ddos-protection protocols gre hbc statistics
<clear-ddos-gre-hbc-statistics>
clear ddos-protection protocols gre punt
<clear-ddos-gre-punt-flows>
clear ddos-protection protocols gre punt states
<clear-ddos-gre-punt-states>
clear ddos-protection protocols gre punt statistics
<clear-ddos-gre-punt-statistics>
clear ddos-protection protocols ipmc-reserved
<clear-ddos-ipmc-reserved-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate
<clear-ddos-ipmc-reserved-aggregate-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate states
<clear-ddos-ipmc-reserved-aggregate-aggregate-states>
clear ddos-protection protocols ipmc-reserved aggregate statistics
<clear-ddos-ipmc-reserved-aggregate-aggregate-statistics>
clear ddos-protection protocols ipmc-reserved culprit-flows
<clear-ddos-ipmc-reserved-aggregate-aggregate-flows>
clear ddos-protection protocols ipmc-reserved aggregate states
<clear-ddos-ipmc-reserved-aggregate-aggregate-states>
clear ddos-protection protocols ipmc-reserved aggregate statistics
<clear-ddos-ipmc-reserved-aggregate-aggregate-statistics>
clear ddos-protection protocols ipmcast-miss
<clear-ddos-ipmcast-miss-aggregate-aggregate-flows>
clear ddos-protection protocols ipmcast-miss aggregate
<clear-ddos-ipmcast-miss-aggregate-aggregate-states>
clear ddos-protection protocols ipmcast-miss aggregate statistics
<clear-ddos-impcast-miss-aggregate-statistics>
clear ddos-protection protocols ipmcast-miss culprit-flows
<clear-ddos-impcast-miss-flows>
clear ddos-protection protocols ipmcast-miss states
<clear-ddos-impcast-miss-states>
clear ddos-protection protocols ipmcast-miss statistics
<clear-ddos-impcast-miss-statistics>
clear ddos-protection protocols l3dest-miss
clear ddos-protection protocols l3dest-miss aggregate
clear ddos-protection protocols l3dest-miss aggregate culprit-flows
<clear-ddos-l3dest-miss-aggregate-flows>
clear ddos-protection protocols l3dest-miss aggregate states
<clear-ddos-l3dest-miss-aggregate-states>
clear ddos-protection protocols l3dest-miss aggregate statistics
<clear-ddos-l3dest-miss-aggregate-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-aggregate-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate states
<clear-ddos-l3mc-sgv-hit-icl-aggregate-states>
clear ddos-protection protocols l3mc-sgv-hit-icl aggregate statistics
<clear-ddos-l3mc-sgv-hit-icl-aggregate-statistics>
clear ddos-protection protocols l3mc-sgv-hit-icl culprit-flows
<clear-ddos-l3mc-sgv-hit-icl-flows>
clear ddos-protection protocols l3mc-sgv-hit-icl states
<clear-ddos-l3mc-sgv-hit-icl-states>
clear ddos-protection protocols l3mc-sgv-hit-icl statistics
<clear-ddos-l3mc-sgv-hit-icl-statistics>
clear ddos-protection protocols l3mtu-fail
clear ddos-protection protocols l3mtu-fail aggregate
clear ddos-protection protocols l3mtu-fail aggregate culprit-flows
<clear-ddos-l3mtu-fail-aggregate-flows>
clear ddos-protection protocols l3mtu-fail aggregate states
<clear-ddos-l3mtu-fail-aggregate-states>
clear ddos-protection protocols 13mtu-fail aggregate statistics
<clear-ddos-13mtu-fail-aggregate-statistics>
clear ddos-protection protocols 13mtu-fail culprit-flows
<clear-ddos-13mtu-fail-flows>
clear ddos-protection protocols 13mtu-fail states
<clear-ddos-13mtu-fail-states>
clear ddos-protection protocols 13mtu-fail statistics
<clear-ddos-13mtu-fail-statistics>
clear ddos-protection protocols 13nhop

clear ddos-protection protocols 13nhop aggregate

clear ddos-protection protocols 13nhop aggregate culprit-flows
<clear-ddos-13nhop-aggregate-flows>
clear ddos-protection protocols 13nhop aggregate states
<clear-ddos-13nhop-aggregate-states>
clear ddos-protection protocols 13nhop aggregate statistics
<clear-ddos-13nhop-aggregate-statistics>
clear ddos-protection protocols 13nhop culprit-flows
<clear-ddos-13nhop-flows>
clear ddos-protection protocols 13nhop states
<clear-ddos-13nhop-states>
clear ddos-protection protocols 13nhop statistics
<clear-ddos-13nhop-statistics>
clear ddos-protection protocols localnh

clear ddos-protection protocols localnh aggregate

clear ddos-protection protocols localnh aggregate culprit-flows
<clear-ddos-localnh-aggregate-flows>
clear ddos-protection protocols localnh aggregate states
<clear-ddos-localnh-aggregate-states>
clear ddos-protection protocols localnh aggregate statistics
<clear-ddos-localnh-aggregate-statistics>
clear ddos-protection protocols localnh culprit-flows
<clear-ddos-localnh-flows>
clear ddos-protection protocols localnh states
<clear-ddos-localnh-states>
clear ddos-protection protocols localnh statistics
<clear-ddos-localnh-statistics>
clear-ddos-dhcpv4-unclass-states

clear-ddos-dhcpv4-unclass-statistics

clear-ddos-dhcpv6-advertise-states

clear-ddos-dhcpv6-advertise-statistics

clear-ddos-dhcpv6-aggregate-states

clear-ddos-dhcpv6-aggregate-statistics
clear-ddos-dhcpv6-confirm-states
clear-ddos-dhcpv6-confirm-statistics
clear-ddos-dhcpv6-decline-states
clear-ddos-dhcpv6-decline-statistics
clear-ddos-dhcpv6-info-req-states
clear-ddos-dhcpv6-info-req-statistics
clear-ddos-dhcpv6-leaseq-da-states
clear-ddos-dhcpv6-leasequery-states
clear-ddos-dhcpv6-leasequery-statistics
clear ddos-protection protocols dhcpv6 leasequery-done
clear ddos-protection protocols dhcpv6 leasequery-done states
clear-ddos-dhcpv6-leaseq-do-states
clear ddos-protection protocols dhcpv6 leasequery-done statistics
clear-ddos-dhcpv6-leaseq-do-statistics
clear ddos-protection protocols dhcpv6 leasequery-reply
clear ddos-protection protocols dhcpv6 leasequery-reply states
clear-ddos-dhcpv6-leaseq-re-states
clear ddos-protection protocols dhcpv6 leasequery-reply statistics
clear-ddos-dhcpv6-leaseq-re-statistics
clear ddos-protection protocols dhcpv6 rebind
clear ddos-protection protocols dhcpv6 rebind states
clear-ddos-dhcpv6-rebind-states
clear ddos-protection protocols dhcpv6 rebind statistics
clear-ddos-dhcpv6-rebind-statistics
clear ddos-protection protocols dhcpv6 reconfigure
clear ddos-protection protocols dhcpv6 reconfigure states
clear-ddos-dhcpv6-reconfig-states
clear ddos-protection protocols dhcpv6 reconfigure statistics
clear-ddos-dhcpv6-reconfig-statistics
clear ddos-protection protocols dhcpv6 relay-forward
clear ddos-protection protocols dhcpv6 relay-forward states
clear-ddos-dhcpv6-relay-for-states
clear ddos-protection protocols dhcpv6 relay-forward statistics
clear-ddos-dhcpv6-relay-for-statistics
clear ddos-protection protocols dhcpv6 relay-reply
clear ddos-protection protocols dhcpv6 relay-reply states
clear-ddos-dhcpv6-relay-rep-states
clear ddos-protection protocols dhcpv6 relay-reply statistics
clear-ddos-dhcpv6-relay-rep-statistics
clear ddos-protection protocols dhcpv6 release
clear ddos-protection protocols dhcpv6 release states
clear-ddos-dhcpv6-release-states
clear ddos-protection protocols dhcpv6 release statistics
clear-ddos-dhcpv6-release-statistics
clear ddos-protection protocols dhcpv6 renew
clear ddos-protection protocols dhcpv6 renew states
clear-ddos-dhcpv6-renew-states
clear ddos-protection protocols dhcpv6 renew statistics
clear-ddos-dhcpv6-renew-statistics
clear ddos-protection protocols dhcpv6 reply
clear ddos-protection protocols dhcpv6 reply states
clear-ddos-dhcpv6-reply-states
clear ddos-protection protocols dhcpv6 reply statistics
clear-ddos-dhcpv6-reply-statistics
clear ddos-protection protocols dhcpv6 request
clear ddos-protection protocols dhcpv6 request culprit-flows
clear ddos-protection protocols dhcpv6 request states
clear-ddos-dhcpv6-request-states
clear ddos-protection protocols dhcpv6 request statistics
clear-ddos-dhcpv6-request-statistics
clear ddos-protection protocols dhcpv6 solicit
clear ddos-protection protocols dhcpv6 solicit culprit-flows
clear ddos-protection protocols dhcpv6 solicit states
clear-ddos-dhcpv6-solicit-states
clear ddos-protection protocols dhcpv6 solicit statistics
clear-ddos-dhcpv6-solicit-statistics
clear ddos-protection protocols dhcpv6 states
clear-ddos-dhcpv6-states
clear ddos-protection protocols dhcpv6 statistics
clear-ddos-dhcpv6-statistics
clear ddos-protection protocols dhcpv6 unclassified
clear ddos-protection protocols dhcpv6 unclassified culprit-flows
clear ddos-protection protocols dhcpv6 unclassified states
clear-ddos-dhcpv6-unclass-states
clear ddos-protection protocols dhcpv6 unclassified statistics
clear-ddos-dhcpv6-unclass-statistics
clear ddos-protection protocols diameter
clear ddos-protection protocols diameter aggregate
clear ddos-protection protocols diameter aggregate culprit-flows
clear ddos-protection protocols diameter aggregate states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-dhcpv6-leaseq-da-statistics
clear-ddos-dhcpv6-leaseq-do-states
clear-ddos-dhcpv6-leaseq-do-statistics
clear-ddos-dhcpv6-leaseq-re-states
clear-ddos-dhcpv6-leaseq-re-statistics
clear-ddos-dhcpv6-rebind-states
clear-ddos-dhcpv6-rebind-statistics
clear-ddos-dhcpv6-reconfig-states
clear-ddos-dhcpv6-reconfig-statistics
clear-ddos-dhcpv6-relay-for-states
clear-ddos-dhcpv6-relay-for-statistics
clear-ddos-dhcpv6-relay-rep-states
clear-ddos-dhcpv6-relay-rep-statistics
clear-ddos-dhcpv6-release-states
clear-ddos-dhcpv6-release-statistics
clear-ddos-dhcpv6-renew-states
clear-ddos-dhcpv6-renew-statistics
clear-ddos-dhcpv6-reply-states
clear-ddos-dhcpv6-reply-statistics
clear-ddos-dhcpv6-request-states
clear-ddos-dhcpv6-request-statistics
clear-ddos-dhcpv6-solicit-states
clear-ddos-dhcpv6-solicit-statistics
clear-ddos-dhcpv6-states
clear-ddos-dhcpv6-statistics
clear-ddos-dhcpv6-unclass-states
clear-ddos-dhcpv6-unclass-statistics
clear-ddos-diameter-aggregate-states
clear ddos-protection protocols diameter aggregate statistics
clear-ddos-diameter-aggregate-statistics
clear ddos-protection protocols diameter states
clear-ddos-diameter-states
clear ddos-protection protocols diameter statistics
clear-ddos-diameter-statistics
clear ddos-protection protocols dns
clear ddos-protection protocols dns aggregate
clear ddos-protection protocols dns aggregate states
clear-ddos-dns-aggregate-states
clear ddos-protection protocols dns aggregate statistics
clear-ddos-dns-aggregate-statistics
clear ddos-protection protocols dns states
clear-ddos-dns-states
clear ddos-protection protocols dns statistics
clear-ddos-dns-statistics
clear ddos-protection protocols dtcp
clear ddos-protection protocols dtcp aggregate
clear ddos-protection protocols dtcp aggregate culprit-flows
clear ddos-protection protocols dtcp aggregate states
clear-ddos-dtcp-aggregate-states
clear ddos-protection protocols dtcp aggregate statistics
clear-ddos-dtcp-aggregate-statistics
clear ddos-protection protocols dtcp states
clear-ddos-dtcp-states
clear ddos-protection protocols dtcp statistics
clear-ddos-dtcp-statistics
clear ddos-protection protocols dynamic-vlan
clear ddos-protection protocols dynamic-vlan aggregate
clear ddos-protection protocols dynamic-vlan aggregate culprit-flows
clear ddos-protection protocols dynamic-vlan aggregate states
clear-ddos-dynvlan-aggregate-states
clear ddos-protection protocols dynamic-vlan aggregate statistics
clear-ddos-dynvlan-aggregate-statistics
clear ddos-protection protocols dynamic-vlan states
clear-ddos-dynvlan-states
clear ddos-protection protocols dynamic-vlan statistics
clear-ddos-dynvlan-statistics
clear ddos-protection protocols egpv6
clear ddos-protection protocols egpv6 aggregate
clear ddos-protection protocols egpv6 aggregate culprit-flows
clear ddos-protection protocols egpv6 aggregate states
clear-ddos-egpv6-aggregate-states
clear ddos-protection protocols egpv6 aggregate statistics
clear-ddos-egpv6-aggregate-statistics
clear ddos-protection protocols egpv6 states
clear-ddos-egpv6-states
clear ddos-protection protocols egpv6 statistics
clear-ddos-egpv6-statistics
clear ddos-protection protocols eoam
clear ddos-protection protocols eoam aggregate
clear ddos-protection protocols eoam aggregate culprit-flows
clear ddos-protection protocols eoam aggregate states
clear-ddos-eoam-aggregate-states
clear ddos-protection protocols eoam aggregate statistics
clear-ddos-eoam-aggregate-statistics
clear ddos-protection protocols eoam states
clear-ddos-eoam-states
clear ddos-protection protocols eoam statistics
clear ddos-protection protocols esmc
clear ddos-protection protocols esmc aggregate
clear ddos-protection protocols esmc aggregate culprit-flows
clear ddos-protection protocols esmc aggregate states
clear ddos-protection protocols esmc aggregate statistics
clear ddos-protection protocols esmc culprit-flows
clear ddos-protection protocols esmc states
clear ddos-protection protocols esmc statistics
<clear-ddos-esmc-statistics>
clear ddos-protection protocols ethernet-tcc
clear ddos-protection protocols ethernet-tcc aggregate
clear ddos-protection protocols ethernet-tcc aggregate culprit-flows
<clear-ddos-eth-tcc-aggregate-flows>
clear ddos-protection protocols ethernet-tcc aggregate states
<clear-ddos-eth-tcc-aggregate-states>
clear ddos-protection protocols ethernet-tcc aggregate statistics
<clear-ddos-eth-tcc-aggregate-statistics>
clear ddos-protection protocols ethernet-tcc culprit-flows
<clear-ddos-eth-tcc-flows>
clear ddos-protection protocols ethernet-tcc states
<clear-ddos-eth-tcc-states>
clear ddos-protection protocols ethernet-tcc statistics
<clear-ddos-eth-tcc-statistics>
clear ddos-protection protocols exceptions
clear ddos-protection protocols exceptions aggregate
clear ddos-protection protocols exceptions aggregate culprit-flows
<clear-ddos-exception-aggregate-flows>
clear ddos-protection protocols exceptions aggregate states
<clear-ddos-exception-aggregate-states>
clear ddos-protection protocols exceptions aggregate statistics
<clear-ddos-exception-aggregate-statistics>
clear ddos-protection protocols exceptions culprit-flows
<clear-ddos-exception-flows>
clear ddos-protection protocols exceptions mcast-rpf-err
clear ddos-protection protocols exceptions mcast-rpf-err culprit-flows
<clear-ddos-exception-mcast-rpf-flows>
clear ddos-protection protocols exceptions mcast-rpf-err states
<clear-ddos-exception-mcast-rpf-states>
clear ddos-protection protocols exceptions mcast-rpf-err statistics
<clear-ddos-exception-mcast-rpf-statistics>
clear ddos-protection protocols exceptions mtu-exceeded
<clear-ddos-exception-mtu-exceed-flows>
clear ddos-protection protocols exceptions mtu-exceeded states
<clear-ddos-exception-mtu-exceed-states>
clear ddos-protection protocols exceptions mtu-exceeded statistics
<clear-ddos-exception-mtu-exceed-statistics>
clear ddos-protection protocols exceptions states
<clear-ddos-exception-states>
clear ddos-protection protocols exceptions statistics
<clear-ddos-exception-statistics>
clear ddos-protection protocols exceptions unclassified
<clear-ddos-exception-unclass-flows>
clear ddos-protection protocols exceptions unclassified states
<clear-ddos-exception-unclass-states>
clear ddos-protection protocols exceptions unclassified statistics
<clear-ddos-exception-unclass-statistics>
clear ddos-protection protocols fab-probe
<clear-ddos-fab-probe-aggregate>
clear ddos-protection protocols fab-probe aggregate states
<clear-ddos-fab-probe-aggregate-states>
clear ddos-protection protocols fab-probe aggregate statistics
<clear-ddos-fab-probe-aggregate-statistics>
clear ddos-protection protocols martian-address
<clear-ddos-martian-address-aggregate-flows>
clear ddos-protection protocols martian-address aggregate states
<clear-ddos-martian-address-aggregate-states>
clear ddos-protection protocols martian-address aggregate statistics
<clear-ddos-martian-address-aggregate-statistics>
clear ddos-protection protocols martian-address culprit-flows
<clear-ddos-martian-address-flows>
clear ddos-protection protocols martian-address states
<clear-ddos-martian-address-states>
clear ddos-protection protocols martian-address statistics
<clear-ddos-martian-address-statistics>
clear-ddos-diameter-statistics
<clear-ddos-dns-aggregate-states>
clear-ddos-dns-aggregate-statistics
<clear-ddos-dns-states>
clear-ddos-dns-statistics
clear-ddos-dtcp-aggregate-states
clear-ddos-dtcp-aggregate-statistics
clear-ddos-dtcp-states
clear-ddos-dtcp-statistics
clear-ddos-dynvlan-aggregate-states
clear-ddos-dynvlan-aggregate-statistics
clear-ddos-dynvlan-states
clear-ddos-dynvlan-statistics
clear-ddos-egpv6-aggregate-states
clear-ddos-egpv6-aggregate-statistics
clear-ddos-egpv6-states
clear-ddos-egpv6-statistics
clear-ddos-eoam-aggregate-states
clear-ddos-eoam-aggregate-statistics
clear-ddos-eoam-states
clear-ddos-eoam-statistics
clear-ddos-esmc-aggregate-states
clear-ddos-esmc-aggregate-statistics
clear-ddos-esmc-states
clear-ddos-esmc-statistics
<clear-ddos-fab-probe-states>
clear ddos-protection protocols fab-probe states
<clear-ddos-fab-probe-states>
clear ddos-protection protocols fab-probe statistics
<clear-ddos-fab-probe-statistics>
clear-ddos-esmc-statistics
clear ddos-protection protocols firewall-host
clear ddos-protection protocols firewall-host aggregate
clear ddos-protection protocols firewall-host aggregate culprit-flows
clear ddos-protection protocols firewall-host aggregate states
clear-ddos-fw-host-aggregate-states
clear ddos-protection protocols firewall-host aggregate statistics
clear ddos-protection protocols firewall-host states
clear ddos-protection protocols firewall-host statistics
clear-ddos-esmc-statistics
clear-ddos-fw-host-aggregate-states
<clear-ddos-fw-host-aggregate-states>
clear-ddos-fw-host-states
<clear-ddos-fw-host-statistics>
clear ddos-protection protocols frame-relay
clear ddos-protection protocols frame-relay aggregate
clear ddos-protection protocols frame-relay aggregate culprit-flows
clear ddos-protection protocols frame-relay aggregate states
clear ddos-protection protocols frame-relay aggregate statistics
clear ddos-protection protocols frame-relay culprit-flows
clear ddos-protection protocols frame-relay frf15
clear ddos-protection protocols frame-relay frf15 culprit-flows
clear ddos-protection protocols frame-relay frf15 states
clear ddos-protection protocols frame-relay frf15 statistics
clear ddos-protection protocols frame-relay frf16
clear ddos-protection protocols frame-relay frf16 culprit-flows
clear ddos-protection protocols frame-relay frf16 states
clear ddos-protection protocols frame-relay frf16 statistics
clear ddos-protection protocols frame-relay states
clear ddos-protection protocols frame-relay statistics
clear ddos-protection protocols ftp
clear ddos-protection protocols ftp aggregate
clear ddos-protection protocols ftp aggregate culprit-flows
clear ddos-protection protocols ftp aggregate states
clear-ddos-ftp-aggregate-states
clear ddos-protection protocols ftp aggregate statistics
clear-ddos-ftp-aggregate-statistics
clear ddos-protection protocols ftp states
clear-ddos-ftp-states
clear ddos-protection protocols ftp statistics
clear-ddos-ftp-statistics
clear ddos-protection protocols ftpv6
clear ddos-protection protocols ftpv6 aggregate
clear ddos-protection protocols ftpv6 aggregate culprit-flows
clear ddos-protection protocols ftpv6 aggregate states
clear-ddos-ftpv6-aggregate-states
clear ddos-protection protocols ftpv6 aggregate statistics
clear-ddos-ftpv6-aggregate-statistics
clear ddos-protection protocols ftpv6 states
clear-ddos-ftpv6-states
clear ddos-protection protocols ftpv6 statistics
clear-ddos-ftpv6-statistics
clear ddos-protection protocols gre
clear ddos-protection protocols gre aggregate
clear ddos-protection protocols gre aggregate culprit-flow
clear ddos-protection protocols gre aggregate states
clear ddos-protection protocols gre aggregate culprit-flows
clear-ddos-ftp-statistics
clear-ddos-ftpv6-aggregate-states
clear-ddos-ftpv6-aggregate-statistics
clear-ddos-ftpv6-states
clear-ddos-ftpv6-statistics
clear-ddos-gre-aggregate-states
clear ddos-protection protocols gre aggregate statistics
clear-ddos-gre-aggregate-statistics
clear ddos-protection protocols gre states
clear-ddos-gre-states
clear ddos-protection protocols gre statistics
clear-ddos-gre-statistics
clear ddos-protection protocols icmp
clear ddos-protection protocols icmp aggregate
clear ddos-protection protocols icmp aggregate states
clear-ddos-icmp-aggregate-states
clear ddos-protection protocols icmp aggregate statistics
clear-ddos-icmp-aggregate-statistics
clear ddos-protection protocols icmp states
clear-ddos-icmp-states
clear ddos-protection protocols icmp statistics
clear-ddos-icmp-statistics
clear ddos-protection protocols icmpv6
clear ddos-protection protocols icmpv6 aggregate
clear ddos-protection protocols icmpv6 aggregate culprit-flows
clear ddos-protection protocols icmpv6 aggregate states
clear-ddos-icmpv6-aggregate-states> clear ddos-protection protocols icmpv6 aggregate states
clear-ddos-icmpv6-aggregate-states> clear ddos-protection protocols icmpv6 aggregate statistics
clear-ddos-icmpv6-aggregate-statistics> clear ddos-protection protocols icmpv6 states
clear-ddos-icmpv6-states> clear ddos-protection protocols icmpv6 statistics
clear-ddos-icmpv6-statistics> clear ddos-protection protocols igmp
clear ddos-protection protocols igmp aggregate
clear ddos-protection protocols igmp aggregate culprit-flows
clear ddos-protection protocols igmp aggregate states
clear-ddos-igmp-aggregate-states
clear ddos-protection protocols igmp aggregate statistics
clear-ddos-igmp-aggregate-statistics
clear ddos-protection protocols igmp states
clear-ddos-igmp-states
clear ddos-protection protocols igmp statistics
clear-ddos-igmp-statistics
clear ddos-protection protocols igmp-snoop
clear ddos-protection protocols igmp-snoop aggregate
clear ddos-protection protocols igmp-snoop aggregate states
clear-ddos-igmp-snoop-aggregate-states
clear ddos-protection protocols igmp-snoop aggregate statistics
clear-ddos-igmp-snoop-aggregate-statistics
clear ddos-protection protocols igmp-snoop states
clear-ddos-igmp-snoop-states
clear ddos-protection protocols igmp-snoop statistics
clear-ddos-igmp-snoop-statistics
clear ddos-protection protocols igmpv4v6
clear ddos-protection protocols igmpv4v6 aggregate
clear ddos-protection protocols igmpv4v6 aggregate states
clear-ddos-igmpv4v6-aggregate-states
clear ddos-protection protocols igmpv4v6 aggregate statistics
clear-ddos-igmpv4v6-aggregate-statistics
clear ddos-protection protocols igmpv4v6 culprit-flows
clear ddos-protection protocols igmpv4v6 states
clear-ddos-igmpv4v6-states
clear ddos-protection protocols igmpv4v6 statistics
clear-ddos-igmpv4v6-statistics
clear ddos-protection protocols igmpv6
clear ddos-protection protocols igmpv6 aggregate
clear ddos-protection protocols igmpv6 aggregate culprit-flows
clear ddos-protection protocols igmpv6 aggregate states
clear ddos-protection protocols igmpv6 aggregate statistics
clear ddos-protection protocols igmpv6 states
clear ddos-protection protocols igmpv6 statistics
<clear-ddos-igmpv6-statistics>clear-ddos-igmp-snoop-states
clear-ddos-igmp-snoop-states
clear-ddos-igmp-snoop-statistics
clear-ddos-igmp-statistics
clear-ddos-igmpv4v6-aggregate-states
clear-ddos-igmpv4v6-aggregate-statistics
clear-ddos-igmpv4v6-states
clear-ddos-igmpv4v6-statistics
clear-ddos-igmpv6-aggregate-states
clear ddos-protection protocols igmpv6 aggregate statistics
clear-ddos-igmpv6-aggregate-statistics
clear ddos-protection protocols igmpv6 states
clear-ddos-igmpv6-states
clear ddos-protection protocols inline-ka
clear ddos-protection protocols inline-ka aggregate
clear ddos-protection protocols inline-ka aggregate culprit-flows
clear ddos-protection protocols inline-ka aggregate states
clear ddos-protection protocols inline-ka aggregate statistics
clear ddos-protection protocols inline-ka culprit-flows
clear ddos-protection protocols inline-ka states
clear ddos-protection protocols inline-ka statistics
clear ddos-protection protocols inline-svcs
clear ddos-protection protocols inline-svcs aggregate
clear ddos-protection protocols inline-svcs aggregate culprit-flows
clear ddos-protection protocols inline-svcs aggregate states
clear ddos-protection protocols inline-svcs aggregate statistics
clear ddos-protection protocols inline-svcs culprit-flows
clear ddos-protection protocols inline-svcs states
clear ddos-protection protocols inline-svcs statistics
clear ddos-protection protocols ip-fragments
clear ddos-protection protocols ip-fragments aggregate
clear ddos-protection protocols ip-fragments aggregate culprit-flows
clear ddos-protection protocols ip-fragments aggregate states
clear ddos-protection protocols ip-fragments aggregate statistics
clear ddos-protection protocols ip-fragments first-fragment
clear ddos-protection protocols ip-fragments first-fragment states
clear ddos-protection protocols ip-fragments first-fragment statistics
clear ddos-protection protocols ip-fragments non-v4v6
clear ddos-protection protocols ip-fragments non-v4v6 states

clear ddos-protection protocols ip-fragments trail-fragment
clear ddos-protection protocols ip-fragments trail-fragment culprit-flows
clear ddos-protection protocols ip-fragments trail-fragment states
clear ddos-protection protocols ip-fragments trail-fragment statistics

clear ddos-protection protocols ip-options
clear ddos-protection protocols ip-options aggregate
clear ddos-protection protocols ip-options aggregate states
clear ddos-protection protocols ip-options non-v4v6
clear ddos-protection protocols ip-options non-v4v6 states
<clear-ddos-ip-opt-non-v4v6-states>
clear-ddos-ip-frag-aggregate-states
clear-ddos-ip-frag-aggregate-statistics
clear-ddos-ip-frag-first-frag-states
clear-ddos-ip-frag-first-frag-statistics
clear-ddos-ip-frag-states
clear-ddos-ip-frag-statistics
clear-ddos-ip-frag-trail-frag-states
clear-ddos-ip-frag-trail-frag-statistics
clear-ddos-ip-opt-aggregate-states
clear-ddos-ip-opt-aggregate-statistics
clear ddos-protection protocols ip-options non-v4v6 statistics
<clear-ddos-ip-opt-non-v4v6-statistics>
clear ddos-protection protocols ip-options router-alert
clear ddos-protection protocols ip-options router-alert culprit-flows
clear ddos-protection protocols ip-options router-alert states
clear-ddos-ip-opt-rt-alert-states
clear ddos-protection protocols ip-options router-alert statistics
clear-ddos-ip-opt-rt-alert-statistics
clear ddos-protection protocols ip-options states
clear-ddos-ip-opt-states
clear ddos-protection protocols ip-options statistics
clear-ddos-ip-opt-statistics
clear ddos-protection protocols ip-options unclassified
clear-ddos-ip-opt-unclass-statistics
clear ddos-protection protocols ipv4-unclassified
clear ddos-protection protocols ipv4-unclassified aggregate
clear-ddos-ipv4-uncls-aggregate-states
clear ddos-protection protocols ipv4-unclassified aggregate statistics
clear-ddos-ipv4-uncls-aggregate-statistics
clear ddos-protection protocols ipv4-unclassified states
clear-ddos-ipv4-uncls-states
clear ddos-protection protocols ipv4-unclassified statistics
clear-ddos-ipv4-uncls-statistics
clear ddos-protection protocols ipv6-unclassified
clear ddos-protection protocols ipv6-unclassified aggregate
clear-ddos-ipv6-uncls-aggregate-states
clear ddos-protection protocols ipv6-unclassified aggregate states
clear-ddos-ipv6-uncls-aggregate-states
clear ddos-protection protocols ipv6-unclassified aggregate statistics
clear-ddos-ipv6-uncls-aggregate-statistics
clear ddos-protection protocols ipv6-unclassified states
clear-ddos-ipv6-uncls-states
clear ddos-protection protocols ipv6-unclassified statistics
clear-ddos-ipv6-uncls-statistics
clear ddos-protection protocols isis
clear-ddos-isis
clear ddos-protection protocols isis aggregate
clear-ddos-isis-aggregate
clear ddos-protection protocols isis aggregate culprit-flows
clear-ddos-isis-aggregate-culprit-flows
clear ddos-protection protocols isis aggregate states
clear-ddos-isis-aggregate-states
clear ddos-protection protocols isis aggregate statistics
<clear-ddos-isis-aggregate-statistics>
clear ddos-protection protocols isis culprit-flows
<clear-ddos-isis-culprit-flows>
clear ddos-protection protocols isis states
<clear-ddos-isis-states>
clear ddos-protection protocols isis statistics
<clear-ddos-isis-statistics>
clear ddos-protection protocols iso-tcc
clear-ddos-isotcc
clear ddos-protection protocols iso-tcc aggregate
<clear-ddos-isotcc-aggregate>
clear ddos-protection protocols iso-tcc aggregate culprit-flows
<clear-ddos-isotcc-aggregate-culprit-flows>
clear ddos-protection protocols iso-tcc aggregate states
<clear-ddos-isotcc-aggregate-states>
clear ddos-protection protocols iso-tcc aggregate statistics
<clear-ddos-isotcc-aggregate-statistics>
clear ddos-protection protocols iso-tcc culprit-flows
<clear-ddos-isotcc-flows>
clear ddos-protection protocols iso-tcc states
<clear-ddos-isotcc-states>
clear ddos-protection protocols iso-tcc statistics
<clear-ddos-isotcc-statistics>
clear ddos-protection protocols jfm
clear-ddos-jfm
clear ddos-protection protocols jfm aggregate
clear-ddos-jfm-aggregate
clear ddos-protection protocols jfm aggregate culprit-flows
<clear-ddos-jfm-aggregate-culprit-flows>
clear ddos-protection protocols jfm aggregate states
clear-ddos-jfm-aggregate-states

clear ddos-protection protocols jfm aggregate statistics
clear-ddos-jfm-aggregate-statistics

clear ddos-protection protocols jfm states
clear-ddos-jfm-states

clear ddos-protection protocols jfm statistics
<clear-ddos-jfm-statistics>

clear ddos-protection protocols keepalive

clear ddos-protection protocols keepalive aggregate

clear ddos-protection protocols keepalive aggregate culprit-flows

clear ddos-protection protocols keepalive aggregate states

clear ddos-protection protocols keepalive aggregate statistics

clear ddos-protection protocols keepalive culprit-flows

clear ddos-protection protocols keepalive states

clear ddos-protection protocols keepalive statistics

clear ddos-protection protocols l2pt

clear ddos-protection protocols l2pt aggregate

clear ddos-protection protocols l2pt aggregate culprit-flows

clear ddos-protection protocols l2pt aggregate states

clear ddos-protection protocols l2pt aggregate statistics

clear ddos-protection protocols l2pt states

clear ddos-protection protocols l2pt statistics

clear ddos-protection protocols l2tp

clear ddos-protection protocols l2tp aggregate

clear ddos-protection protocols l2tp aggregate culprit-flows

clear ddos-protection protocols l2tp aggregate states

clear-ddos-l2tp-aggregate-states

clear ddos-protection protocols l2tp aggregate statistics

clear-ddos-l2tp-aggregate-statistics

clear ddos-protection protocols l2tp states

clear ddos-protection protocols l2tp statistics

clear ddos-protection protocols lacp

clear ddos-protection protocols lacp aggregate

clear ddos-protection protocols lacp aggregate culprit-flows

clear ddos-protection protocols lacp aggregate states

clear-ddos-lacp-aggregate-states

clear ddos-protection protocols lacp aggregate statistics

clear-ddos-lacp-aggregate-statistics

clear ddos-protection protocols lacp states
clear-ddos-lacp-states
clear ddos-protection protocols lacp statistics
clear-ddos-lacp-statistics
clear ddos-protection protocols ldp
clear ddos-protection protocols ldp aggregate
clear ddos-protection protocols ldp aggregate culprit-flows
clear ddos-protection protocols ldp aggregate states
clear-ddos-isis-states
clear-ddos-isis-statistics
clear-ddos-jfm-aggregate-states
clear-ddos-jfm-aggregate-statistics
clear-ddos-jfm-states
clear-ddos-l2tp-aggregate-states
clear-ddos-l2tp-aggregate-statistics
clear-ddos-l2tp-states
clear-ddos-l2tp-statistics
clear-ddos-lacp-aggregate-states
clear-ddos-lacp-aggregate-statistics
clear-ddos-lacp-states
clear-ddos-lacp-statistics
clear-ddos-ldp-aggregate-states
clear-ddos-ldp-aggregate-statistics
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp aggregate statistics
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp culprit-flows
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp states
clear ddos-protection protocols ldp statistics
clear ddos-protection protocols ldp statistics
clear-ddos-ldp-aggregate-statistics
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate culprit-flows
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate states
clear ddos-protection protocols ldpv6 aggregate statistics
clear ddos-protection protocols ldpv6 aggregate statistics
clear-ddos-ldpv6-aggregate-statistics
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 states
clear ddos-protection protocols ldpv6 statistics
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate culprit-flows
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate states
clear ddos-protection protocols lldp aggregate statistics
clear ddos-protection protocols lldp aggregate statistics

clear ddos-protection protocols lmp
clear ddos-protection protocols lmp
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate culprit-flows
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate statistics
clear ddos-protection protocols lmp aggregate states
clear ddos-protection protocols lmp aggregate states

clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate culprit-flows
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate states
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 aggregate statistics
clear ddos-protection protocols lmpv6 aggregate states

1076
clear ddos-protection protocols lmpv6 culprit-flows
clear ddos-protection protocols lmpv6 states
clear-ddos-lmpv6-states
clear ddos-protection protocols lmpv6 statistics
clear-ddos-lmpv6-statistics
clear ddos-protection protocols mac-host
clear ddos-protection protocols mac-host aggregate
clear ddos-protection protocols mac-host aggregate culprit-flows
clear ddos-protection protocols mac-host aggregate states
clear-ddos-mac-host-aggregate-states
clear ddos-protection protocols mac-host aggregate statistics
clear-ddos-mac-host-aggregate-statistics
clear ddos-protection protocols mac-host states
clear-ddos-mac-host-states
clear ddos-protection protocols mac-host statistics
clear ddos-protection protocols mcast-snoop
clear ddos-protection protocols mcast-snoop aggregate
clear ddos-protection protocols mcast-snoop aggregate culprit-flows
clear ddos-protection protocols mcast-snoop aggregate states
clear ddos-protection protocols mcast-snoop aggregate statistics
clear ddos-protection protocols mcast-snoop culprit-flows
clear ddos-protection protocols mcast-snoop igmp
clear ddos-protection protocols mcast-snoop igmp culprit-flows
<clear-ddos-mcast-snoop-igmp-flows>
clear ddos-protection protocols mcast-snoop igmp states
<clear-ddos-mcast-snoop-igmp-states>
clear ddos-protection protocols mcast-snoop igmp statistics
<clear-ddos-mcast-snoop-igmp-statistics>
clear ddos-protection protocols mcast-snoop mld
clear ddos-protection protocols mcast-snoop mld culprit-flows
<clear-ddos-mcast-snoop-mld-flows>
clear ddos-protection protocols mcast-snoop mld states
<clear-ddos-mcast-snoop-mld-states>
clear ddos-protection protocols mcast-snoop mld statistics
<clear-ddos-mcast-snoop-mld-statistics>
clear ddos-protection protocols mld
clear ddos-protection protocols mld aggregate
clear ddos-protection protocols mld aggregate culprit-flows
<clear-ddos-mld-aggregate-flows>
clear ddos-protection protocols mld aggregate states
<clear-ddos-mld-aggregate-states>
clear ddos-protection protocols mld aggregate statistics
<clear-ddos-mld-aggregate-statistics>
clear ddos-protection protocols mld culprit-flows
<clear-ddos-mld-flows>
clear ddos-protection protocols mld states
<clear-ddos-mld-states>
clear ddos-protection protocols mld statistics
<clear-ddos-mld-statistics>
clear ddos-protection protocols mlp
clear ddos-protection protocols mlp add
clear ddos-protection protocols mlp add culprit-flows
<clear-ddos-mlp-add-flows>
clear ddos-protection protocols mlp add states
<clear-ddos-mlp-add-states>
clear ddos-protection protocols mlp add statistics
<clear-ddos-mlp-add-statistics>
clear ddos-protection protocols mlp aggregate
clear ddos-protection protocols mlp aggregate culprit-flows
clear ddos-protection protocols mlp aggregate states
<clear-ddos-mlp-aggregate-states>
clear ddos-protection protocols mlp aggregate statistics
<clear-ddos-mlp-aggregate-statistics>
clear ddos-protection protocols mlp aging-exception
clear ddos-protection protocols mlp aging-exception culprit-flows
clear ddos-protection protocols mlp aging-exception states
<clear-ddos-mlp-aging-exc-states>
clear ddos-protection protocols mlp aging-exception statistics
<clear-ddos-mlp-aging-exc-statistics>
clear ddos-protection protocols mlp packets
clear ddos-protection protocols mlp packets states
<clear-ddos-mlp-packets-states>
clear ddos-protection protocols mlp packets statistics
<clear-ddos-mlp-packets-statistics>
clear ddos-protection protocols mlp macpin-exception
clear ddos-protection protocols mlp macpin-exception culprit-flows
<clear-ddos-mlp-mac-pinning-flows>
clear ddos-protection protocols mlp macpin-exception states
<clear-ddos-mlp-mac-pinning-states>
clear ddos-protection protocols mlp macpin-exception statistics
<clear-ddos-mlp-mac-pinning-statistics>
clear ddos-protection protocols mlp states
<clear-ddos-mlp-states>
clear ddos-protection protocols mlp statistics
<clear-ddos-mlp-statistics>
clear-ddos-mlp-statistics
clear ddos-protection protocols mlp unclassified
clear ddos-protection protocols mlp unclassified states
clear-ddos-mlp-unclass-states
clear ddos-protection protocols mlp unclassified statistics
clear-ddos-mlp-unclass-statistics
clear ddos-protection protocols msdp
clear ddos-protection protocols msdp aggregate
clear ddos-protection protocols msdp aggregate states
clear-ddos-msdp-aggregate-states
clear ddos-protection protocols msdp aggregate statistics
clear-ddos-msdp-aggregate-statistics
clear ddos-protection protocols msdp culprit-flows
clear ddos-protection protocols msdp states
clear-ddos-msdp-states
clear ddos-protection protocols msdp statistics
clear-ddos-msdp-statistics
clear ddos-protection protocols msdpv6
clear ddos-protection protocols msdpv6 aggregate
clear ddos-protection protocols msdpv6 aggregate culprit-flows
clear ddos-protection protocols msdpv6 aggregate states
clear-ddos-msdpv6-aggregate-states
clear ddos-protection protocols msdpv6 aggregate statistics
clear-ddos-msdpv6-aggregate-statistics
clear ddos-protection protocols msdpv6 states
clear-ddos-msdpv6-states
clear ddos-protection protocols msdpv6 statistics
clear-ddos-msdpv6-statistics
clear ddos-protection protocols multicast-copy
clear ddos-protection protocols multicast-copy aggregate
clear ddos-protection protocols multicast-copy aggregate states
clear-ddos-mcast-copy-aggregate-states
clear ddos-protection protocols multicast-copy aggregate statistics
clear-ddos-mcast-copy-aggregate-statistics
clear ddos-protection protocols multicast-copy states
clear-ddos-mcast-copy-states
clear ddos-protection protocols multicast-copy statistics
clear-ddos-mcast-copy-statistics
clear ddos-protection protocols mvrp
clear ddos-protection protocols mvrp aggregate
clear ddos-protection protocols mvrp aggregate states
clear-ddos-mvrp-aggregate-states
clear ddos-protection protocols mvrp aggregate statistics
clear ddos-protection protocols mvrp culprit-flows
clear ddos-protection protocols mvrp states
clear-ddos-mvrp-states
clear ddos-protection protocols mvrp statistics
clear-ddos-mvrp-statistics
clear ddos-protection protocols ndpv6
clear ddos-protection protocols ndpv6 aggregate
clear ddos-protection protocols ndpv6 aggregate states
clear ddos-protection protocols ndpv6 aggregate statistics
clear ddos-protection protocols ndpv6 neighbor-advertisement
clear ddos-protection protocols ndpv6 neighbor-advertisement culprit-flows
<clear-ddos-ndpv6-neighb-adv-flows>
clear ddos-protection protocols ndpv6 neighbor-advertisement states
<clear-ddos-ndpv6-neighb-adv-states>
clear ddos-protection protocols ndpv6 neighbor-advertisement statistics
<clear-ddos-ndpv6-neighb-adv-statistics>
clear ddos-protection protocols ndpv6 neighbor-solicitation
clear ddos-protection protocols ndpv6 neighbor-solicitation culprit-flows
<clear-ddos-ndpv6-neighb-sol-flows>
clear ddos-protection protocols ndpv6 neighbor-solicitation states
<clear-ddos-ndpv6-neighb-sol-states>
clear ddos-protection protocols ndpv6 neighbor-solicitation statistics
<clear-ddos-ndpv6-neighb-sol-statistics>
clear ddos-protection protocols ndpv6 redirect
clear ddos-protection protocols ndpv6 redirect culprit-flows
<clear-ddos-ndpv6-redirect-flows>
clear ddos-protection protocols ndpv6 redirect states
<clear-ddos-ndpv6-redirect-states>
clear ddos-protection protocols ndpv6 redirect statistics
<clear-ddos-ndpv6-redirect-statistics>
clear ddos-protection protocols ndpv6 router-advertisement
clear ddos-protection protocols ndpv6 router-advertisement culprit-flows
<clear-ddos-ndpv6-router-adv-flows>
clear ddos-protection protocols ndpv6 router-advertisement states
<clear-ddos-ndpv6-router-adv-states>
clear ddos-protection protocols ndpv6 router-advertisement statistics
<clear-ddos-ndpv6-router-adv-statistics>
clear ddos-protection protocols ndpv6 router-solicitation
clear ddos-protection protocols ndpv6 router-solicitation culprit-flows
<clear-ddos-ndpv6-router-sol-flows>
clear ddos-protection protocols ndpv6 router-solicitation states
<clear-ddos-ndpv6-router-sol-states>
clear ddos-protection protocols ndpv6 router-solicitation statistics
<clear-ddos-ndpv6-router-sol-statistics>
clear ddos-protection protocols ndpv6 states
clear ddos-protection protocols ndpv6 statistics
clear ddos-protection protocols nonucast-switch
clear ddos-protection protocols nonucast-switch aggregate
clear ddos-protection protocols nonucast-switch aggregate culprit-flows
<clear-ddos-nonucast-switch-aggregate-flows>
clear ddos-protection protocols nonucast-switch aggregate states
<clear-ddos-nonucast-switch-aggregate-states>
clear ddos-protection protocols nonucast-switch aggregate statistics
<clear-ddos-nonucast-switch-aggregate-statistics>
clear ddos-protection protocols nonucast-switch culprit-flows
<clear-ddos-nonucast-switch-flows>
clear ddos-protection protocols nonucast-switch states
<clear-ddos-nonucast-switch-states>
clear ddos-protection protocols nonucast-switch statistics
<clear-ddos-nonucast-switch-statistics>
clear ddos-protection protocols ntp aggregate
clear ddos-protection protocols ntp aggregate states
<clear-ddos-ntp-aggregate-states>
clear ddos-protection protocols ntp aggregate statistics
<clear-ddos-ntp-aggregate-statistics>
clear ddos-protection protocols ntp culprit-flows
clear ddos-protection protocols ntp states
clear-ddos-ntp-states
clear ddos-protection protocols ntp statistics
clear-ddos-ntp-statistics
clear ddos-protection protocols oam-cfm
clear ddos-protection protocols oam-cfm aggregate
clear ddos-protection protocols oam-cfm aggregate culprit-flows
<clear-ddos-oam-cfm-aggregate-flows>
clear ddos-protection protocols oam-cfm aggregate states
<clear-ddos-oam-cfm-aggregate-states>
clear ddos-protection protocols oam-cfm aggregate statistics
<clear-ddos-oam-cfm-aggregate-statistics>
clear ddos-protection protocols oam-cfm culprit-flows
<clear-ddos-oam-cfm-flows>
clear ddos-protection protocols oam-cfm states
<clear-ddos-oam-cfm-states>
clear ddos-protection protocols oam-cfm statistics
<clear-ddos-oam-cfm-statistics>
clear ddos-protection protocols oam-lfm
clear ddos-protection protocols ldp-hello aggregate
clear ddos-protection protocols ldp-hello aggregate culprit-flows
<clear-ddos-ldp-hello-aggregate-flows>
clear ddos-protection protocols ldp-hello aggregate states
<clear-ddos-ldp-hello-aggregate-states>
clear ddos-protection protocols ldp-hello aggregate statistics
<clear-ddos-ldp-hello-aggregate-statistics>
clear ddos-protection protocols ldp-hello culprit-flows
<clear-ddos-ldp-hello-flows>
clear ddos-protection protocols ldp-hello states
<clear-ddos-ldp-hello-states>
clear ddos-protection protocols ldp-hello statistics
<clear-ddos-ldp-hello-statistics>
clear-ddos-ldp-statistics
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-states
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-aggregate-statistics
clear-ddos-ldpv6-states
clear-ddos-ldpv6-states
clear-ddos-ldpv6-statistics
clear-ddos-ldpv6-statistics
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-states
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-aggregate-statistics
clear-ddos-lldp-states
clear-ddos-lldp-states
clear-ddos-lldp-statistics
clear-ddos-lldp-statistics
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-states
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-aggregate-statistics
clear-ddos-lmp-states
clear-ddos-lmp-states
clear-ddos-lmp-statistics
clear-ddos-lmp-statistics
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-aggregate-states
clear-ddos-lmpv6-states
clear-ddos-lmpv6-states
clear-ddos-lmpv6-statistics
clear-ddos-mac-host-aggregate-states
clear-ddos-mac-host-aggregate-statistics
clear-ddos-mac-host-states
clear-ddos-mac-host-statistics
common-ddos-mcast-copy-aggregate-states
common-ddos-mcast-copy-aggregate-statistics
common-ddos-mcast-copy-states
common-ddos-mcast-copy-statistics
common-ddos-mlp-aggregate-states
common-ddos-mlp-aggregate-statistics
common-ddos-mlp-aging-exc-states
common-ddos-mlp-aging-exc-statistics
common-ddos-mlp-packets-states
common-ddos-mlp-packets-statistics
common-ddos-mlp-states
common-ddos-mlp-statistics
common-ddos-mlp-unclass-states
common-ddos-mlp-unclass-statistics
common-ddos-msdp-aggregate-states
common-ddos-msdp-aggregate-statistics
common-ddos-msdp-states
common-ddos-msdp-statistics
common-ddos-msdpv6-aggregate-states
common-ddos-msdpv6-aggregate-statistics
common-ddos-msdpv6-states
common-ddos-msdpv6-statistics
common-ddos-protection protocols multihop-bfd
common-ddos-protection protocols multihop-bfd aggregate
common-ddos-protection protocols multihop-bfd aggregate culprit-flows
<common-ddos-mhop-bfd-aggregate-flows>
common-ddos-protection protocols multihop-bfd aggregate states
<common-ddos-mhop-bfd-aggregate-states>
common-ddos-protection protocols multihop-bfd aggregate statistics
<common-ddos-mhop-bfd-aggregate-statistics>
common-ddos-protection protocols multihop-bfd culprit-flows
<common-ddos-mhop-bfd-flows>
common-ddos-protection protocols multihop-bfd states
<common-ddos-mhop-bfd-states>
common-ddos-protection protocols multihop-bfd statistics
<common-ddos-mhop-bfd-statistics>
common-ddos-mvrp-aggregate-states
clear-ddos-mvrp-aggregate-statistics
clear-ddos-mvrp-states
clear-ddos-mvrp-statistics
clear-ddos-ntp-aggregate-states
clear-ddos-ntp-aggregate-statistics
clear-ddos-ntp-states
clear-ddos-ntp-statistics
clear-ddos-oam-lfm-aggregate-states
clear-ddos-oam-lfm-aggregate-statistics
clear-ddos-oam-lfm-states
clear-ddos-oam-lfm-statistics
clear-ddos-ospf-aggregate-states
clear-ddos-ospf-aggregate-statistics
clear-ddos-ospf-states
clear-ddos-ospf-statistics
clear-ddos-ospf3v6-aggregate-states
clear-ddos-ospf3v6-aggregate-statistics
clear ddos-protection protocols ospf3v6 aggregate statistics
clear-ddos-ospf3v6-states
clear ddos-protection protocols pimv6
clear-ddos-pim-statistics
clear ddos-protection protocols pim-ctrl
clear ddos-protection protocols pim-ctrl aggregate
<clear-ddos-pim-ctrl-aggregate-flows>
clear ddos-protection protocols pim-ctrl aggregate culprit-flows
<clear-ddos-pim-ctrl-aggregate-states>
clear ddos-protection protocols pim-ctrl aggregate statistics
<clear-ddos-pim-ctrl-aggregate-statistics>
clear ddos-protection protocols pim-ctrl culprit-flows
<clear-ddos-pim-ctrl-flows>
clear ddos-protection protocols pim-ctrl states
<clear-ddos-pim-ctrl-states>
clear ddos-protection protocols pim-ctrl statistics
<clear-ddos-pim-ctrl-statistics>
clear ddos-protection protocols pim-data
clear ddos-protection protocols pim-data aggregate
clear ddos-protection protocols pim-data aggregate culprit-flows
<clear-ddos-pim-data-aggregate-flows>
clear ddos-protection protocols pim-data aggregate states
<clear-ddos-pim-data-aggregate-states>
clear ddos-protection protocols pim-data aggregate statistics
<clear-ddos-pim-data-aggregate-statistics>
clear ddos-protection protocols pim-data culprit-flows
<clear-ddos-pim-data-flows>
clear ddos-protection protocols pim-data states
<clear-ddos-pim-data-states>
clear ddos-protection protocols pim-data statistics
<clear-ddos-pim-data-statistics>
clear ddos-protection protocols pfe-alive
clear ddos-protection protocols pfe-alive aggregate
clear ddos-protection protocols pfe-alive aggregate states
clear-ddos-pfe-alive-aggregate-states
clear ddos-protection protocols pfe-alive aggregate statistics
clear ddos-protection protocols pfe-alive culprit-flows
clear-ddos-pfe-alive-flows
clear ddos-protection protocols pfe-alive states
<clear-ddos-pfe-alive-states>
clear ddos-protection protocols pfe-alive statistics
<clear-ddos-pfe-alive-statistics>
clear ddos-protection protocols pim
clear ddos-protection protocols pim aggregate
clear ddos-protection protocols pim aggregate states
<clear-ddos-pim-aggregate-states>
clear ddos-protection protocols pim aggregate statistics
clear ddos-protection protocols pim culprit-flows
<clear-ddos-pim-flows>
clear ddos-protection protocols pim states
<clear-ddos-pim-states>
clear ddos-protection protocols pim statistics
<clear-ddos-pim-statistics>
clear ddos-protection protocols pimv6
clear ddos-protection protocols pimv6 aggregate
<clear-ddos-pimv6-aggregate-flows>
clear ddos-protection protocols pimv6 aggregate culprit-flows
<clear-ddos-pimv6-aggregate-states>
clear ddos-protection protocols pimv6 aggregate statistics
<clear-ddos-pimv6-aggregate-statistics>
clear ddos-protection protocols pimv6 states
<clear-ddos-pimv6-states>
clear ddos-protection protocols pkt-inject
clear ddos-protection protocols pkt-inject aggregate
<clear-ddos-pkt-inject-aggregate-flows>
clear ddos-protection protocols pkt-inject aggregate states
<clear-ddos-pkt-inject-aggregate-states>
clear ddos-protection protocols pkt-inject aggregate statistics
clear ddos-protection protocols pkt-inject culprit-flows
<clear-ddos-pkt-inject-flows>
clear ddos-protection protocols pkt-inject states
<clear-ddos-pkt-inject-states>
clear ddos-protection protocols pkt-inject statistics
<clear-ddos-pkt-inject-statistics>
clear ddos-protection protocols pmvrp aggregate
<clear-ddos-pmvrp-aggregate>
clear ddos-protection protocols pmvrp aggregate states
<clear-ddos-pmvrp-aggregate-states>
clear ddos-protection protocols pmvrp aggregate statistics
<clear-ddos-pmvrp-aggregate-statistics>
clear ddos-protection protocols pmvrp culprit-flows
<clear-ddos-pmvrp-culprit-flows>
clear ddos-protection protocols pos aggregate
<clear-ddos-pos-aggregate>
clear ddos-protection protocols pos aggregate states
<clear-ddos-pos-aggregate-states>
clear ddos-protection protocols pos aggregate statistics
<clear-ddos-pos-aggregate-statistics>
clear ddos-protection protocols pos states
<clear-ddos-pos-states>
clear ddos-protection protocols pos statistics
<clear-ddos-pos-statistics>
clear ddos-protection protocols ppp aggregate
<clear-ddos-ppp-aggregate>
clear ddos-protection protocols ppp aggregate states
<clear-ddos-ppp-aggregate-states>
clear ddos-protection protocols ppp aggregate statistics
<clear-ddos-ppp-aggregate-statistics>
clear ddos-protection protocols ppp authentication
<clear-ddos-ppp-auth>
clear ddos-protection protocols ppp authentication states
<clear-ddos-ppp-auth-states>
clear ddos-protection protocols ppp authentication statistics
<clear-ddos-ppp-auth-statistics>
clear-ddos-ppp-auth-statistics
clear ddos-protection protocols ppp ipcp
clear ddos-protection protocols ppp ipcp states
clear-ddos-ppp-ipcp-states
clear ddos-protection protocols ppp ipcp statistics
clear-ddos-ppp-ipcp-statistics
clear ddos-protection protocols ppp ipv6cp
clear ddos-protection protocols ppp ipv6cp states
clear-ddos-ppp-ipv6cp-states
clear ddos-protection protocols ppp ipv6cp statistics
clear-ddos-ppp-ipv6cp-statistics
clear ddos-protection protocols ppp isis
clear ddos-protection protocols ppp isis states
clear-ddos-ppp-isis-states
clear ddos-protection protocols ppp isis statistics
clear-ddos-ppp-isis-statistics
clear ddos-protection protocols ppp lcp
clear ddos-protection protocols ppp lcp states
clear-ddos-ppp-lcp-states
clear ddos-protection protocols ppp lcp statistics
clear-ddos-ppp-lcp-statistics
clear ddos-protection protocols ppp mplscp
clear ddos-protection protocols ppp mplscp states
clear-ddos-ppp-mplscp-states
clear ddos-protection protocols ppp mplscp statistics
clear-ddos-ppp-mplscp-statistics
clear ddos-protection protocols ppp states
clear-ddos-ppp-states
clear ddos-protection protocols ppp statistics
clear-ddos-ppp-statistics
clear ddos-protection protocols ppp unclassified
clear ddos-protection protocols ppp unclassified states
clear ddos-protection protocols ppp unclassified statistics
<clear-ddos-ppp-unclass-statistics>
clear ddos-protection protocols pppoe
clear ddos-protection protocols pppoe aggregate
clear ddos-protection protocols pppoe aggregate states
clear-ddos-pppoe-aggregate-states
clear ddos-protection protocols pppoe aggregate statistics
clear-ddos-pppoe-aggregate-statistics
clear ddos-protection protocols pppoe padi
clear ddos-protection protocols pppoe padi states
clear-ddos-pppoe-padi-states
clear ddos-protection protocols pppoe padi statistics
clear-ddos-pppoe-padi-statistics
clear ddos-protection protocols pppoe padm
clear ddos-protection protocols pppoe padm states
clear-ddos-pppoe-padm-states
clear ddos-protection protocols pppoe padm statistics
clear-ddos-pppoe-padm-statistics
clear ddos-protection protocols pppoe padn
clear ddos-protection protocols pppoe padn states
clear-ddos-pppoe-padn-states
clear ddos-protection protocols pppoe padn statistics
clear-ddos-pppoe-padn-statistics
clear ddos-protection protocols pppoe pado
clear ddos-protection protocols pppoe pado states
clear-ddos-pppoe-pado-states
clear ddos-protection protocols pppoe pado statistics
clear-ddos-pppoe-pado-statistics
clear ddos-protection protocols pppoe padr
clear ddos-protection protocols pppoe padr states
clear-ddos-pppoe-padr-states
clear ddos-protection protocols pppoe padr statistics
clear-ddos-pppoe-padr-statistics
clear ddos-protection protocols pppoe pads
clear ddos-protection protocols pppoe pads states
clear-ddos-pppoe-pads-states
clear ddos-protection protocols pppoe pads statistics
clear-ddos-pppoe-pads-statistics
clear ddos-protection protocols pppoe padt
clear ddos-protection protocols pppoe padt states
clear-ddos-pppoe-padt-states
clear ddos-protection protocols pppoe padt statistics
clear-ddos-pppoe-padt-statistics
clear ddos-protection protocols pppoe states
clear-ddos-pppoe-states
clear ddos-protection protocols pppoe statistics
clear-ddos-pppoe-statistics
clear ddos-protection protocols proto-802-1x
clear ddos-protection protocols proto-802-1x aggregate
clear ddos-protection protocols proto-802-1x aggregate culprit-flows
<clear-ddos-8021x-aggregate-flows>
clear ddos-protection protocols proto-802-1x aggregate states
<clear-ddos-8021x-aggregate-states>
clear ddos-protection protocols proto-802-1x aggregate statistics
<clear-ddos-8021x-aggregate-statistics>
clear ddos-protection protocols proto-802-1x culprit-flows
<clear-ddos-8021x-flows>
clear ddos-protection protocols proto-802-1x states
<clear-ddos-8021x-states>
clear ddos-protection protocols proto-802-1x statistics
<clear-ddos-8021x-statistics>
clear ddos-protection protocols ptp
<clear-ddos-ptp-aggregate-states>
clear ddos-protection protocols ptp aggregate
<clear-ddos-ptp-aggregate-statistics>
clear ddos-protection protocols ptp aggregate states
<clear-ddos-ptp-aggregate-states>
clear ddos-protection protocols ptp aggregate statistics
<clear-ddos-ptp-aggregate-statistics>
clear ddos-protection protocols ptp states
<clear-ddos-ptp-states>
clear ddos-protection protocols ptp statistics
<clear-ddos-ptp-statistics>
clear ddos-protection protocols ptpv6
<clear-ddos-tpv6-aggregate-statistics>
clear ddos-protection protocols ptpv6 aggregate
<clear-ddos-tpv6-aggregate-states>
clear ddos-protection protocols ptpv6 aggregate statistics
<clear-ddos-tpv6-aggregate-states>
clear ddos-protection protocols ptpv6 aggregate culprit-flows
<clear-ddos-tpv6-aggregate-flows>
clear ddos-protection protocols ptpv6 aggregate states
<clear-ddos-tpv6-aggregate-states>
clear ddos-protection protocols ptpv6 aggregate statistics
<clear-ddos-tpv6-aggregate-statistics>
clear ddos-protection protocols ptpv6 culprit-flows
<clear-ddos-tpv6-flows>
clear ddos-protection protocols ptpv6 states
<clear-ddos-tpv6-states>
clear ddos-protection protocols ptpv6 statistics
<clear-ddos-tpv6-statistics>
clear ddos-protection protocols pvstp
<clear-ddos-pvstp-aggregate-states>
clear ddos-protection protocols pvstp aggregate
<clear-ddos-pvstp-aggregate-statistics>
clear ddos-protection protocols pvstp aggregate states
<clear-ddos-pvstp-aggregate-states>
clear ddos-protection protocols pvstp aggregate statistics
<clear-ddos-pvstp-aggregate-statistics>
clear ddos-protection protocols pvstp states
<clear-ddos-pvstp-states>
clear ddos-protection protocols pvstp statistics
clear-ddos-pvstp-statistics
clear ddos-protection protocols radius
clear ddos-protection protocols radius accounting
clear ddos-protection protocols radius accounting states
clear-ddos-radius-account-states
clear ddos-protection protocols radius accounting statistics
clear-ddos-radius-account-statistics
clear ddos-protection protocols radius aggregate
clear ddos-protection protocols radius aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius aggregate statistics
clear-ddos-radius-aggregate-statistics
clear ddos-protection protocols radius authorization
clear ddos-protection protocols radius authorization states
clear ddos-protection protocols radius authorization statistics
clear-ddos-radius-authorization-statistics
clear ddos-protection protocols radius ospfv3v6
clear ddos-protection protocols radius ospfv3v6 aggregate
clear ddos-protection protocols radius ospfv3v6 aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius ospfv3v6 aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius ospfv3v6 accounting
clear ddos-protection protocols radius ospfv3v6 accounting states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius ospfv3v6 accounting statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius pmvrf
clear ddos-protection protocols radius pmvrf aggregate
clear ddos-protection protocols radius pmvrf aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius pmvrf aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius pos
clear ddos-protection protocols radius pos aggregate
clear ddos-protection protocols radius pos aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius pos aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius ppp
clear ddos-protection protocols radius ppp aggregate
clear ddos-protection protocols radius ppp aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius ppp aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius ppp ipcp
clear ddos-protection protocols radius ppp ipcp aggregate
clear ddos-protection protocols radius ppp ipcp aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius ppp ipcp aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius ipv6cp
clear ddos-protection protocols radius ipv6cp aggregate
clear ddos-protection protocols radius ipv6cp aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius ipv6cp aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius isis
clear ddos-protection protocols radius isis aggregate
clear ddos-protection protocols radius isis aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius isis aggregate statistics
clear-ddos-radius-aggregate-statistics

clear ddos-protection protocols radius lcp
clear ddos-protection protocols radius lcp aggregate
clear ddos-protection protocols radius lcp aggregate states
clear-ddos-radius-aggregate-states
clear ddos-protection protocols radius lcp aggregate statistics
clear-ddos-radius-aggregate-statistics

1091
clear-ddos-ppp-mplscp-states
clear-ddos-ppp-mplscp-statistics

clear-ddos-pppoe-aggregate-states
clear-ddos-pppoe-aggregate-statistics

clear-ddos-pppoe-padi-states
clear-ddos-pppoe-padi-statistics

clear-ddos-pppoe-padm-states
clear-ddos-pppoe-padm-statistics

clear-ddos-pppoe-padn-states
clear-ddos-pppoe-padn-statistics

clear-ddos-pppoe-pado-states
clear-ddos-pppoe-pado-statistics

clear-ddos-pppoe-padr-states
clear-ddos-pppoe-padr-statistics

clear-ddos-pppoe-pads-states
clear-ddos-pppoe-pads-statistics

clear-ddos-pppoe-padt-states
clear-ddos-pppoe-padt-statistics

clear-ddos-pppoe-states

clear-ddos-pppoe-statistics

clear-ddos-ppp-states

clear-ddos-ppp-statistics

clear-ddos-ptp-aggregate-states

clear-ddos-ptp-aggregate-statistics

clear-ddos-ptp-states

clear-ddos-ptp-statistics

clear-ddos-pvstp-aggregate-states

clear-ddos-pvstp-aggregate-statistics

clear-ddos-pvstp-states

clear-ddos-pvstp-statistics

clear-ddos-radius-account-states

clear-ddos-radius-account-statistics

clear-ddos-radius-aggregate-states

clear-ddos-radius-aggregate-statistics

clear-ddos-radius-auth-states

clear-ddos-radius-auth-statistics

clear ddos-protection protocols radius authorization statistics

clear ddos-protection protocols pmvrp culprit-flows

clear ddos-protection protocols radius server

clear ddos-protection protocols radius server states

clear-ddos-radius-server-states

clear ddos-protection protocols radius server statistics
clear-ddos-radius-server-statistics
clear ddos-protection protocols radius states
clear-ddos-radius-states
clear ddos-protection protocols radius statistics
clear-ddos-radius-statistics
clear ddos-protection protocols redirect
clear ddos-protection protocols redirect aggregate
clear ddos-protection protocols redirect aggregate states
clear-ddos-redirect-aggregate-states
clear ddos-protection protocols redirect aggregate statistics
clear-ddos-redirect-aggregate-statistics
clear ddos-protection protocols redirect states
clear-ddos-redirect-states
clear ddos-protection protocols redirect statistics
clear-ddos-redirect-statistics
clear ddos-protection protocols reject
clear ddos-protection protocols reject aggregate
clear ddos-protection protocols reject aggregate states
clear ddos-protection protocols reject aggregate statistics
clear ddos-protection protocols reject states
clear ddos-protection protocols reject statistics
clear ddos-protection protocols rip
clear ddos-protection protocols rip aggregate
clear ddos-protection protocols rip aggregate states
clear-ddos-rip-aggregate-states
clear ddos-protection protocols rip aggregate statistics
clear-ddos-rip-aggregate-statistics
clear ddos-protection protocols rip states
clear-ddos-rip-states
clear ddos-protection protocols rip statistics
clear-ddos-rip-statistics
clear ddos-protection protocols ripv6
clear ddos-protection protocols ripv6 aggregate
clear ddos-protection protocols ripv6 aggregate states
clear-ddos-ripv6-aggregate-states
clear ddos-protection protocols ripv6 aggregate statistics
clear-ddos-ripv6-aggregate-statistics
clear ddos-protection protocols ripv6 states
clear-ddos-ripv6-states
clear ddos-protection protocols ripv6 statistics
clear-ddos-ripv6-statistics
clear ddos-protection protocols rsvp
clear ddos-protection protocols rsvp aggregate
clear ddos-protection protocols rsvp aggregate states
clear-ddos-rsvp-aggregate-states
clear ddos-protection protocols rsvp aggregate statistics
clear-ddos-rsvp-aggregate-statistics
clear ddos-protection protocols rsvp states
clear-ddos-rsvp-states
clear ddos-protection protocols rsvp statistics
clear-ddos-rsvp-statistics
clear ddos-protection protocols rsvpv6
clear ddos-protection protocols rsvpv6 aggregate
clear ddos-protection protocols rsvpv6 aggregate states
clear-ddos-rsvpv6-aggregate-states
clear ddos-protection protocols rsvpv6 aggregate statistics
clear-ddos-rsvpv6-aggregate-statistics
clear ddos-protection protocols rsvpv6 states
clear-ddos-rsvpv6-states
clear ddos-protection protocols rsvpv6 statistics
clear-ddos-rsvpv6-statistics
clear ddos-protection protocols sample
clear ddos-protection protocols sample aggregate
clear ddos-protection protocols sample aggregate states
<clear-ddos-sample-aggregate-states>
clear ddos-protection protocols sample aggregate statistics
<clear-ddos-sample-aggregate-statistics>
clear ddos-protection protocols sample host
clear ddos-protection protocols sample host states
<clear-ddos-sample-host-states>
clear ddos-protection protocols sample host statistics
<clear-ddos-sample-host-statistics>
clear ddos-protection protocols sample pfe
clear ddos-protection protocols sample pfe culprit-flows
clear ddos-protection protocols sample pfe states
<clear-ddos-sample-pfe-states>
clear ddos-protection protocols sample pfe statistics
clear ddos-protection protocols sample sflow
clear ddos-protection protocols sample sflow culprit-flows
<clear-ddos-sample-sflow-flows>
clear ddos-protection protocols sample sflow states
<clear-ddos-sample-sflow-states>
clear ddos-protection protocols sample sflow statistics
<clear-ddos-sample-sflow-statistics>
clear ddos-protection protocols sample states
<clear-ddos-sample-states>
clear ddos-protection protocols sample statistics
<clear-ddos-sample-statistics>
clear ddos-protection protocols sample syslog
clear ddos-protection protocols sample syslog culprit-flows
clear ddos-protection protocols sample syslog states
<clear-ddos-sample-syslog-states>
clear ddos-protection protocols sample syslog statistics
<clear-ddos-sample-syslog-statistics>
clear ddos-protection protocols sample tap
clear ddos-protection protocols sample tap states
<clear-ddos-sample-tap-states>
clear ddos-protection protocols sample tap statistics
<clear-ddos-sample-tap-statistics>
clear ddos-protection protocols sample-dest aggregate
<clear-ddos-sample-dest-aggregate-flows>
clear ddos-protection protocols sample-dest aggregate states
<clear-ddos-sample-dest-aggregate-states>
clear ddos-protection protocols sample-dest aggregate statistics
<clear-ddos-sample-dest-aggregate-statistics>
clear ddos-protection protocols sample-dest culprit-flows
<clear-ddos-sample-dest-flows>
clear ddos-protection protocols sample-dest states
<clear-ddos-sample-dest-states>
clear ddos-protection protocols sample-dest statistics
<clear-ddos-sample-dest-statistics>
clear ddos-protection protocols sample-source aggregate
<clear-ddos-sample-source-aggregate-flows>
clear ddos-protection protocols sample-source aggregate states
<clear-ddos-sample-source-aggregate-states>
clear ddos-protection protocols sample-source aggregate statistics
<clear-ddos-sample-source-aggregate-statistics>
clear ddos-protection protocols sample-source culprit-flows
<clear-ddos-sample-source-flows>
clear ddos-protection protocols sample-source states
<clear-ddos-sample-source-states>
clear ddos-protection protocols sample-source statistics
<clear-ddos-sample-source-statistics>
clear ddos-protection protocols sample tap statistics
<clear-ddos-sample-tap-statistics>
clear ddos-protection protocols services
clear ddos-protection protocols services aggregate
<clear-ddos-services-aggregate>
clear ddos-protection protocols services aggregate states
<clear-ddos-services-aggregate-states>
clear ddos-protection protocols services aggregate statistics
<clear-ddos-services-aggregate-statistics>
clear ddos-protection protocols services bsdt
<clear-ddos-services-BSDT>
clear ddos-protection protocols services bsdt culprit-flows
<clear-ddos-services-BSDT-flows>
clear ddos-protection protocols services bsdt states
<clear-ddos-services-BSDT-states>
clear ddos-protection protocols services bsdt statistics
<clear-ddos-services-BSDT-statistics>
clear ddos-protection protocols services packet
<clear-ddos-services-flows>
clear ddos-protection protocols services packet culprit-flows
<clear-ddos-services-packet-flows>
clear ddos-protection protocols services packet states
<clear-ddos-services-packet-states>
clear ddos-protection protocols services packet statistics
<clear-ddos-services-packet-statistics>
clear ddos-protection protocols services states
<clear-ddos-services-states>
clear ddos-protection protocols services statistics
<clear-ddos-services-statistics>
clear ddos-protection protocols snmp
<clear-ddos-services-SNMP>
clear ddos-protection protocols snmp aggregate
<clear-ddos-services-SNMP-aggregate>
clear ddos-protection protocols snmp aggregate states
<clear-ddos-services-SNMP-aggregate-states>
clear ddos-protection protocols snmp aggregate statistics
<clear-ddos-services-SNMP-aggregate-statistics>
clear ddos-protection protocols snmp culprit-flows
<clear-ddos-services-SNMP-flows>
clear ddos-protection protocols snmp states
<clear-ddos-services-SNMP-states>
clear ddos-protection protocols snmp statistics
<clear-ddos-services-SNMP-statistics>
clear ddos-protection protocols snmpv6
<clear-ddos-services-SNMPv6>
clear ddos-protection protocols snmpv6 aggregate
<clear-ddos-services-SNMPv6-aggregate>
clear ddos-protection protocols snmpv6 aggregate states
<clear-ddos-services-SNMPv6-aggregate-states>
clear ddos-protection protocols snmpv6 aggregate statistics
<clear-ddos-services-SNMPv6-aggregate-statistics>
clear ddos-protection protocols snmpv6 states
<clear-ddos-services-SNMPv6-states>
clear-ddos-snmpv6-states
clear ddos-protection protocols snmpv6 statistics
clear-ddos-snmpv6-statistics

clear ddos-protection protocols ssh
clear ddos-protection protocols ssh aggregate
clear ddos-protection protocols ssh aggregate states

clear-ddos-ssh-aggregate-states
clear ddos-protection protocols ssh aggregate statistics

clear-ddos-ssh-aggregate-statistics

clear ddos-protection protocols ssh states

clear-ddos-ssh-states


clear ddos-protection protocols ssh statistics

clear-ddos-ssh-statistics

clear ddos-protection protocols sshv6
clear ddos-protection protocols sshv6 aggregate
clear ddos-protection protocols sshv6 aggregate states

clear-ddos-sshv6-aggregate-states
clear ddos-protection protocols sshv6 aggregate statistics

clear-ddos-sshv6-aggregate-statistics

clear ddos-protection protocols sshv6 culprit-flows

clear ddos-protection protocols sshv6 states

clear-ddos-sshv6-states


clear ddos-protection protocols sshv6 statistics

clear-ddos-sshv6-statistics

clear ddos-protection protocols states

clear-ddos-protocols-states

clear ddos-protection protocols statistics

clear-ddos-protocols-statistics

clear ddos-protection protocols stp
clear ddos-protection protocols stp aggregate
clear ddos-protection protocols stp aggregate states

clear-ddos-stp-aggregate-states
clear ddos-protection protocols stp aggregate statistics

clear-ddos-stp-aggregate-statistics

clear ddos-protection protocols stp states

clear-ddos-stp-states


clear ddos-protection protocols stp statistics

clear-ddos-stp-statistics

clear ddos-protection protocols tacacs
clear ddos-protection protocols tacacs aggregate
clear ddos-protection protocols tacacs aggregate states

clear-ddos-tacacs-aggregate-states

clear ddos-protection protocols tacacs aggregate statistics
clear-ddos-tacacs-aggregate-statistics
clear ddos-protection protocols tacacs states
clear-ddos-tacacs-states
clear ddos-protection protocols tacacs statistics
clear-ddos-tacacs-statistics
clear ddos-protection protocols tcc
clear ddos-protection protocols tcc aggregate
clear ddos-protection protocols tcc aggregate culprit-flows
<clear-ddos-tcc-aggregate-flows>
clear ddos-protection protocols tcc aggregate states
<clear-ddos-tcc-aggregate-states>
clear ddos-protection protocols tcc aggregate statistics
<clear-ddos-tcc-aggregate-statistics>
clear ddos-protection protocols tcc culprit-flows
<clear-ddos-tcc-flows>
clear ddos-protection protocols tcc ethernet-tcc
clear ddos-protection protocols tcc ethernet-tcc culprit-flows
<clear-ddos-tcc-ethernet-tcc-flows>
clear ddos-protection protocols tcc ethernet-tcc states
<clear-ddos-tcc-ethernet-tcc-states>
clear ddos-protection protocols tcc ethernet-tcc statistics
<clear-ddos-tcc-ethernet-tcc-statistics>
clear ddos-protection protocols tcc iso-tcc
clear ddos-protection protocols tcc iso-tcc culprit-flows
<clear-ddos-tcc-iso-tcc-flows>
clear ddos-protection protocols tcc iso-tcc states
<clear-ddos-tcc-iso-tcc-states>
clear ddos-protection protocols tcc iso-tcc statistics
<clear-ddos-tcc-iso-tcc-statistics>
clear ddos-protection protocols tcc states
<clear-ddos-tcc-states>
clear ddos-protection protocols tcc statistics
<clear-ddos-tcc-statistics>
clear ddos-protection protocols tcc unclassified
clear ddos-protection protocols tcc unclassified culprit-flows
<clear-ddos-tcc-unclass-flows>
clear ddos-protection protocols tcc unclassified states
<clear-ddos-tcc-unclass-states>
clear ddos-protection protocols tcc unclassified statistics
<clear-ddos-tcc-unclass-statistics>
clear ddos-protection protocols tcp-flags
clear ddos-protection protocols tcp-flags aggregate
clear ddos-protection protocols tcp-flags aggregate states
clear-ddos-tcp-flags-aggregate-states
clear ddos-protection protocols tcp-flags aggregate statistics
clear-ddos-tcp-flags-aggregate-statistics
clear ddos-protection protocols tcp-flags established
clear-ddos-tcp-flags-establish-states
clear ddos-protection protocols tcp-flags established statistics
clear-ddos-tcp-flags-establish-statistics
clear ddos-protection protocols tcp-flags initial culprit-flows
clear-ddos-tcp-flags-initial-culprit-flows
clear ddos-protection protocols tcp-flags initial states
clear-ddos-tcp-flags-initial-states
clear ddos-protection protocols tcp-flags initial statistics
clear-ddos-tcp-flags-initial-statistics
clear ddos-protection protocols tcp-flags states
clear-ddos-tcp-flags-states
clear ddos-protection protocols tcp-flags statistics
clear-ddos-tcp-flags-statistics
clear ddos-protection protocols tcp-flags unclassified
clear-ddos-tcp-flags-unclass-states
clear ddos-protection protocols tcp-flags unclassified states
clear-ddos-tcp-flags-unclass-statistics
clear ddos-protection protocols telnet
clear-ddos-telnet-states
clear ddos-protection protocols telnet statistics
clear-ddos-telnet-statistics
clear ddos-protection protocols telnetv6
clear-ddos-telnetv6-states
clear-ddos-telnetv6-states
clear ddos-protection protocols telnetv6 statistics
clear-ddos-telnetv6-statistics
clear ddos-protection protocols ttl
clear ddos-protection protocols ttl aggregate
clear ddos-protection protocols ttl aggregate culprit-flows
clear ddos-protection protocols ttl aggregate states
clear-ddos-ttl-aggregate-states
clear ddos-protection protocols ttl aggregate statistics
clear-ddos-ttl-aggregate-statistics
clear ddos-protection protocols ttl states
clear-ddos-ttl-states
clear ddos-protection protocols ttl statistics
clear-ddos-ttl-statistics
clear ddos-protection protocols tunnel-fragment
clear ddos-protection protocols tunnel-fragment aggregate
clear ddos-protection protocols tunnel-fragment aggregate states
clear-ddos-tun-frag-aggregate-states
clear ddos-protection protocols tunnel-fragment aggregate statistics
clear-ddos-tun-frag-aggregate-statistics
clear ddos-protection protocols tunnel-fragment states
clear-ddos-tun-frag-states
clear ddos-protection protocols tunnel-fragment statistics
clear-ddos-tun-frag-statistics
clear ddos-protection protocols unclassified
clear ddos-protection protocols unclassified aggregate
clear ddos-protection protocols unclassified aggregate states
clear ddos-protection protocols unclassified aggregate statistics
clear ddos-protection protocols unclassified control-layer2
clear ddos-protection protocols unclassified control-layer2 culprit-flows
clear ddos-protection protocols unclassified control-layer2 states
clear ddos-protection protocols unclassified control-layer2 statistics
clear ddos-protection protocols unclassified control-v4
clear ddos-protection protocols unclassified control-v4 culprit-flows
clear ddos-protection protocols unclassified control-v4 states
clear ddos-protection protocols unclassified control-v4 statistics
clear ddos-protection protocols unclassified control-v6
clear ddos-protection protocols unclassified control-v6 culprit-flows
clear ddos-protection protocols unclassified control-v6 states
clear ddos-protection protocols unclassified control-v6 statistics
clear ddos-protection protocols unclassified filter-v4 culprit-flows
clear ddos-protection protocols unclassified filter-v4 states
clear ddos-protection protocols unclassified filter-v4 statistics
clear ddos-protection protocols unclassified filter-v6
clear ddos-protection protocols unclassified filter-v6 culprit-flows
clear ddos-protection protocols unclassified filter-v6 states
clear ddos-protection protocols unclassified filter-v6 statistics
clear ddos-protection protocols unclassified fw-host
clear ddos-protection protocols unclassified fw-host culprit-flows
<clear-ddos-uncls-fw-host-flows>
<clear-ddos-uncls-fw-host-states>
clear ddos-protection protocols unclassified fw-host statistics
<clear-ddos-uncls-fw-host-statistics>
clear ddos-protection protocols unclassified host-route-v4
clear ddos-protection protocols unclassified host-route-v4 culprit-flows
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 states
clear ddos-protection protocols unclassified host-route-v4 statistics
clear ddos-protection protocols unclassified host-route-v6
clear ddos-protection protocols unclassified host-route-v6 culprit-flows
clear ddos-protection protocols unclassified host-route-v6 states
clear ddos-protection protocols unclassified host-route-v6 states
clear ddos-protection protocols unclassified host-route-v6 statistics
clear ddos-protection protocols unclassified mcast-copy
clear ddos-protection protocols unclassified mcast-copy culprit-flows
<clear-ddos-uncls-mcast-copy-flows>
clear ddos-protection protocols unclassified mcast-copy states
<clear-ddos-uncls-mcast-copy-states>
clear ddos-protection protocols unclassified mcast-copy statistics
<clear-ddos-uncls-mcast-copy-statistics>
clear ddos-protection protocols unknown-l2mc
clear ddos-protection protocols unknown-l2mc aggregate
clear ddos-protection protocols unknown-l2mc aggregate culprit-flows
<clear-ddos-unknown-l2mc-aggregate-flows>
clear ddos-protection protocols unknown-l2mc aggregate states
<clear-ddos-unknown-l2mc-aggregate-states>
clear ddos-protection protocols unknown-l2mc aggregate statistics
<clear-ddos-unknown-l2mc-aggregate-statistics>
clear ddos-protection protocols unknown-l2mc culprit-flows
<clear-ddos-unknown-l2mc-flows>
clear ddos-protection protocols unknown-l2mc states
<clear-ddos-unknown-l2mc-states>
clear ddos-protection protocols unknown-l2mc statistics
<clear-ddos-unknown-l2mc-statistics>
clear ddos-protection protocols urpf-fail
clear ddos-protection protocols urpf-fail aggregate
<clear-ddos-urpf-fail-aggregate-flows>
clear ddos-protection protocols urpf-fail aggregate states
<clear-ddos-urpf-fail-aggregate-states>
clear ddos-protection protocols urpf-fail aggregate statistics
<clear-ddos-urpf-fail-aggregate-statistics>
clear ddos-protection protocols urpf-fail culprit-flows
<clear-ddos-urpf-fail-flows>
clear ddos-protection protocols urpf-fail states
<clear-ddos-urpf-fail-states>
clear ddos-protection protocols urpf-fail statistics
<clear-ddos-urpf-fail-statistics>
clear ddos-protection protocols vcipc-udp
clear ddos-protection protocols vcipc-udp aggregate
<clear-ddos-vcipc-udp-aggregate-flows>
clear ddos-protection protocols vcipc-udp aggregate states
<clear-ddos-vcipc-udp-aggregate-states>
clear ddos-protection protocols vcipc-udp aggregate statistics
<clear-ddos-vcipc-udp-aggregate-statistics>
clear ddos-protection protocols vcipc-udp culprit-flows
<clear-ddos-vcipc-udp-flows>
clear ddos-protection protocols vcipc-udp states
<clear-ddos-vcipc-udp-states>
clear ddos-protection protocols vcipc-udp-statistics
<clear-ddos-uncls-statistics>
clear ddos-protection protocols unclassified other
clear ddos-protection protocols unclassified other culprit-flows
clear ddos-protection protocols unclassified other states
clear ddos-protection protocols unclassified other statistics
clear ddos-protection protocols unclassified resolve-v4
clear ddos-protection protocols unclassified resolve-v4 culprit-flows
clear ddos-protection protocols unclassified resolve-v4 states
clear ddos-protection protocols unclassified resolve-v4 statistics
clear ddos-protection protocols unclassified resolve-v6
clear ddos-protection protocols unclassified resolve-v6 culprit-flows
clear ddos-protection protocols unclassified resolve-v6 states
clear ddos-protection protocols unclassified resolve-v6 statistics
clear ddos-protection protocols unclassified states
clear ddos-protection protocols unclassified statistics
clear ddos-protection protocols virtual-chassis
clear ddos-protection protocols virtual-chassis aggregate
clear ddos-protection protocols virtual-chassis aggregate culprit-flows
clear ddos-protection protocols virtual-chassis aggregate states
clear-ddos-protocols-states
clear-ddos-protocols-statistics
clear-ddos-radius-server-states
clear-ddos-radius-server-statistics
clear-ddos-radius-states
clear-ddos-radius-statistics
clear ddos-protection protocols re-services
  clear ddos-protection protocols re-services aggregate
clear ddos-protection protocols re-services aggregate culprit-flows
  <clear-ddos-re-services-aggregate-flows>
clear ddos-protection protocols re-services aggregate states
  <clear-ddos-re-services-aggregate-states>
clear ddos-protection protocols re-services aggregate statistics
  <clear-ddos-re-services-aggregate-statistics>
clear ddos-protection protocols re-services captive-portal
clear ddos-protection protocols re-services captive-portal culprit-flows
  <clear-ddos-re-services-captive-portal-flows>
clear ddos-protection protocols re-services captive-portal states
  <clear-ddos-re-services-captive-portal-states>
clear ddos-protection protocols re-services captive-portal statistics
  <clear-ddos-re-services-captive-portal-statistics>
clear ddos-protection protocols re-services culprit-flows
  <clear-ddos-re-services-flows>
clear ddos-protection protocols re-services states
  <clear-ddos-re-services-states>
clear ddos-protection protocols re-services statistics
  <clear-ddos-re-services-statistics>
clear ddos-protection protocols re-services-v6
clear ddos-protection protocols re-services-v6 aggregate
clear ddos-protection protocols re-services-v6 aggregate culprit-flows
  <clear-ddos-re-services-v6-aggregate-flows>
clear ddos-protection protocols re-services-v6 aggregate states
  <clear-ddos-re-services-v6-aggregate-states>
clear ddos-protection protocols re-services-v6 aggregate statistics
  <clear-ddos-re-services-v6-aggregate-statistics>
clear ddos-protection protocols re-services-v6 captive-portal
clear ddos-protection protocols re-services-v6 captive-portal culprit-flows
  <clear-ddos-re-services-v6-captive-portal-v6-flows>
clear ddos-protection protocols re-services-v6 captive-portal states
<clear-ddos-re-services-v6-captive-portal-v6-states>
clear ddos-protection protocols re-services-v6 captive-portal statistics
<clear-ddos-re-services-v6-captive-portal-v6-statistics>
clear ddos-protection protocols re-services-v6 culprit-flows
<clear-ddos-re-services-v6-flows>
clear ddos-protection protocols re-services-v6 states
<clear-ddos-re-services-v6-states>
clear ddos-protection protocols re-services-v6 statistics
<clear-ddos-re-services-v6-statistics>
clear ddos-redirect-aggregate-states
<clear-ddos-redirect-aggregate-states>
clear ddos-redirect-states
<clear-ddos-redirect-states>
clear ddos-redirect-statistics
<clear-ddos-redirect-statistics>
clear ddos-rip-aggregate-states
<clear-ddos-rip-aggregate-states>
clear ddos-rip-states
<clear-ddos-rip-states>
clear ddos-rip-statistics
<clear-ddos-rip-statistics>
clear ddos-ripv6-aggregate-states
<clear-ddos-ripv6-aggregate-states>
clear ddos-ripv6-states
<clear-ddos-ripv6-states>
clear ddos-ripv6-statistics
<clear-ddos-ripv6-statistics>
clear ddos-rsvp-aggregate-states
<clear-ddos-rsvp-aggregate-states>
clear ddos-rsvp-states
<clear-ddos-rsvp-states>
clear ddos-rsvp-statistics
<clear-ddos-rsvp-statistics>
clear ddos-rsvpv6-aggregate-states
<clear-ddos-rsvpv6-aggregate-states>
clear ddos-rsvpv6-states
<clear-ddos-rsvpv6-states>
clear ddos-rsvpv6-statistics
<clear-ddos-rsvpv6-statistics>
clear ddos-services-aggregate-states
<clear-ddos-services-aggregate-states>
clear ddos-services-states
<clear-ddos-services-states>
clear ddos-services-statistics
<clear-ddos-services-statistics>
clear ddos-snmp-aggregate-states
<clear-ddos-snmp-aggregate-states>
clear ddos-snmp-states
<clear-ddos-snmp-states>
clear ddos-snmp-statistics
<clear-ddos-snmp-statistics>
clear ddos-snmpv6-aggregate-states
<clear-ddos-snmpv6-aggregate-states>
clear ddos-snmpv6-states
<clear-ddos-snmpv6-states>
clear ddos-snmpv6-statistics
<clear-ddos-snmpv6-statistics>
clear ddos-ssh-aggregate-states
clear-ddos-ssh-aggregate-statistics
clear-ddos-ssh-states
clear-ddos-ssh-statistics
clear-ddos-sshv6-aggregate-states
clear-ddos-sshv6-aggregate-statistics
clear-ddos-sshv6-states
clear-ddos-sshv6-statistics
clear-ddos-stp-aggregate-states
clear-ddos-stp-aggregate-statistics
clear-ddos-stp-states
clear-ddos-stp-statistics
clear ddos-protection protocols syslog
clear ddos-protection protocols syslog aggregate
clear ddos-protection protocols syslog aggregate culprit-flows
<clear-ddos-syslog-aggregate-flows>
clear ddos-protection protocols syslog aggregate states
<clear-ddos-syslog-aggregate-states>
clear ddos-protection protocols syslog aggregate statistics
<clear-ddos-syslog-aggregate-statistics>
clear ddos-protection protocols syslog culprit-flows
<clear-ddos-syslog-flows>
clear ddos-protection protocols syslog states
<clear-ddos-syslog-states>
clear ddos-protection protocols syslog statistics
<clear-ddos-syslog-statistics>
clear-ddos-tacacs-aggregate-states
clear-ddos-tacacs-aggregate-statistics
clear-ddos-tacacs-states
clear-ddos-tacacs-statistics
clear-ddos-tcp-flags-aggregate-states
clear-ddos-tcp-flags-aggregate-statistics
clear-ddos-tcp-flags-establish-states
clear-ddos-tcp-flags-establish-statistics
clear-ddos-tcp-flags-initial-states
clear-ddos-tcp-flags-initial-statistics
clear-ddos-tcp-flags-states
clear-ddos-tcp-flags-statistics
clear-ddos-tcp-flags-unclass-states
clear-ddos-tcp-flags-unclass-statistics
clear-ddos-telnet-aggregate-states
clear-ddos-telnet-aggregate-statistics
clear-ddos-telnet-states
clear-ddos-telnet-statistics
clear-ddos-telnetv6-aggregate-states
clear-ddos-telnetv6-aggregate-statistics
clear-ddos-telnetv6-states
clear-ddos-telnetv6-statistics
clear-ddos-ttl-aggregate-states
clear-ddos-ttl-aggregate-statistics
clear-ddos-ttl-states
clear-ddos-ttl-statistics
clear-ddos-tun-frag-aggregate-states
clear-ddos-tun-frag-aggregate-statistics
clear-ddos-tun-frag-states
clear-ddos-tun-frag-statistics
clear ddos-protection protocols tunnel-ka
clear ddos-protection protocols tunnel-ka aggregate
clear ddos-protection protocols tunnel-ka aggregate culprit-flows
<clear-ddos-tunnel-ka-aggregate-flows>
clear ddos-protection protocols tunnel-ka aggregate states
<clear-ddos-tunnel-ka-aggregate-states>
clear ddos-protection protocols tunnel-ka aggregate statistics
<clear-ddos-tunnel-ka-aggregate-statistics>
clear ddos-protection protocols tunnel-ka culprit-flows
<clear-ddos-tunnel-ka-flows>
clear ddos-protection protocols tunnel-ka states
<clear-ddos-tunnel-ka-states>
clear ddos-protection protocols tunnel-ka statistics
<clear-ddos-tunnel-ka-statistics>
clear-ddos-vchassis-aggregate-states
clear ddos-protection protocols virtual-chassis aggregate statistics
clear-ddos-vchassis-aggregate-statistics
clear ddos-protection protocols virtual-chassis control-high
clear ddos-protection protocols virtual-chassis control-high states
clear-ddos-vchassis-control-hi-states
clear ddos-protection protocols virtual-chassis control-high statistics
clear-ddos-vchassis-control-hi-statistics
clear ddos-protection protocols virtual-chassis control-low
clear ddos-protection protocols virtual-chassis control-low states
clear-ddos-vchassis-control-lo-states
clear ddos-protection protocols virtual-chassis control-low statistics
clear-ddos-vchassis-control-lo-statistics
clear ddos-protection protocols virtual-chassis states
clear-ddos-vchassis-states
clear ddos-protection protocols virtual-chassis statistics
clear-ddos-vchassis-statistics
clear ddos-protection protocols virtual-chassis unclassified
clear ddos-protection protocols virtual-chassis unclassified culprit-flows
clear ddos-protection protocols virtual-chassis unclassified states
clear-ddos-vchassis-unclass-states
clear ddos-protection protocols virtual-chassis unclassified statistics
clear-ddos-vchassis-unclass-statistics
clear ddos-protection protocols virtual-chassis vc-packets
clear-ddos-vchassis-vc-packets
clear ddos-protection protocols virtual-chassis vc-packets states
clear-ddos-vchassis-vc-packets-states
clear ddos-protection protocols virtual-chassis vc-packets statistics
clear-ddos-vchassis-vc-packets-statistics
clear ddos-protection protocols virtual-chassis vc-ttl-errors
clear-ddos-vchassis-vc-ttl-errors
clear ddos-protection protocols virtual-chassis vc-ttl-errors states
clear-ddos-vchassis-vc-ttl-err-states
clear ddos-protection protocols virtual-chassis vc-ttl-errors statistics
clear-ddos-vchassis-vc-ttl-err-statistics
clear ddos-protection protocols vrrp
clear ddos-protection protocols vrrp aggregate
clear ddos-protection protocols vrrp aggregate states
clear-ddos-vrrp-aggregate-states
clear ddos-protection protocols vrrp aggregate statistics
clear-ddos-vrrp-aggregate-statistics
clear ddos-protection protocols vrrp culprit-flows
clear-ddos-vrrp-statistics
clear ddos-protection protocols vrrpv6
clear ddos-protection protocols vrrpv6 aggregate
clear ddos-protection protocols vrrpv6 aggregate states
clear-ddos-vrrpv6-aggregate-states
clear ddos-protection protocols vrrpv6 aggregate statistics
clear-ddos-vrrpv6-aggregate-statistics
clear ddos-protection protocols vrrpv6 states
clear-ddos-vrrpv6-states
clear ddos-protection protocols vrrpv6 statistics
clear-ddos-uncls-host-rt-v4-flows
clear-ddos-vchassis-aggregate-statistics
clear-ddos-vchassis-control-hi-states
clear-ddos-vchassis-control-hi-statistics
clear-ddos-vchassis-control-lo-states
clear-ddos-vchassis-control-lo-statistics
clear-ddos-vchassis-states
clear-ddos-vchassis-statistics
clear-ddos-vchassis-unclass-states
clear-ddos-vchassis-unclass-statistics
clear-ddos-vchassis-vc-packets-states
clear-ddos-vchassis-vc-packets-statistics
clear-ddos-vchassis-vc-ttl-err-states
clear-ddos-vchassis-vc-ttl-err-statistics
clear-ddos-vrrp-aggregate-states
clear-ddos-vrrp-aggregate-statistics
clear-ddos-vrrp-states
clear-ddos-vrrp-statistics
clear-ddos-vrrpv6-aggregate-states
clear-ddos-vrrpv6-aggregate-statistics
clear-ddos-vrrpv6-states
clear-ddos-vrrpv6-statistics
clear ddos-protection protocols vxlan
clear ddos-protection protocols vxlan aggregate
clear ddos-protection protocols vxlan aggregate culprit-flows
clear ddos-vxlan-aggregate-flows
clear ddos-protection protocols vxlan aggregate states
<clear-ddos-vxlan-aggregate-states>
clear ddos-protection protocols vxlan aggregate statistics
<clear-ddos-vxlan-aggregate-statistics>
clear ddos-protection protocols vxlan culprit-flows
<clear-ddos-vxlan-flows>
clear ddos-protection protocols vxlan states
<clear-ddos-vxlan-states>
clear ddos-protection protocols vxlan statistics
<clear-ddos-vxlan-statistics>
clear dhcp
clear dhcp client
clear dhcp client binding
<clear-dhcp-client-binding-information>
clear dhcp client statistics
<clear-client-statistics-information>
clear dhcp proxy-client
clear dhcp proxy-client statistics
clear dhcp relay
clear dhcp relay binding
<clear-dhcp-relay-binding-information>
clear dhcp relay binding interface
<clear-dhcp-interface-bindings>
clear dhcp relay statistics
  <clear-dhcp-relay-statistics-information>
  <clear-dhcp-security-binding>
  <clear-dhcp-security-binding-interface>
  <clear-dhcp-security-binding-ip-address>
  <clear-dhcp-security-binding-statistics>
  <clear-dhcp-security-binding-vlan>
  clear dhcp relay statistics bulk-leasequery-connections
  <clear-dhcp-relay-bulk-leasequery-conn-statistics>
  clear dhcp relay statistics leasequery
  <clear-dhcp-relay-leasequery-statistics>
  clear dhcp server
  clear dhcp server binding
  <clear-dhcp-server-binding-information>
  clear dhcp server binding interface
  <clear-dhcp-server-binding-interface>
  clear dhcp server statistics
  <clear-server-statistics-information>
  clear dhcp statistics
  <clear-dhcp-service-statistics-information>
  clear dhcp-security statistics
  <clear-dhcp-security-statistics>
  clear dhcpv6
  clear dhcpv6 client
  clear dhcpv6 client binding
  <clear-dhcpv6-client-binding-information>
  clear dhcpv6 client statistics
  <clear-dhcpv6-client-statistics-information>
  clear dhcpv6 proxy-client
  clear dhcpv6 proxy-client statistics
  <clear-dhcpv6-proxy-client-statistics-information>
  clear dhcpv6 relay
  clear dhcpv6 relay binding
  clear dhcpv6 relay binding interface
  clear dhcpv6 relay statistics
  <clear-dhcpv6-relay-statistics-information>
  clear dhcpv6 relay statistics bulk-leasequery-connections
  <clear-dhcpv6-relay-bulk-leasequery-conn-statistics>
  clear dhcpv6 relay statistics leasequery
  <clear-dhcpv6-relay-leasequery-statistics>
  clear dhcpv6 server
  clear dhcpv6 server binding
<clear-dhcpv6-server-binding-information>
clear dhcpv6 server binding interface
<clear-dhcpv6-server-binding-interface>
clear dhcpv6 server statistics
<clear-dhcpv6-server-statistics-information>
clear dhcpv6 server statistics bulk-leasequery-connections
<clear-dhcpv6-server-bulk-leasequery-statistics>
clear dhcpv6 statistics
<clear-dhcpv6-service-statistics-information>
clear diameter
<clear-diameter>
clear diameter function
<clear-diameter-function>
clear diameter peer
<clear-diameter-peer>
<clear-dhcp-binding-information>
<clear-dhcp-conflict-information>
<clear-dhcp-statistics-information>
clear system subscriber-management
<clear-subscriber-management>
clear system subscriber-management arp
<clear-subscriber-management-arp>
clear system subscriber-management arp address
<clear-subscriber-management-arp-address>
clear system subscriber-management arp interface
<clear-subscriber-management-arp-interface>
clear system subscriber-management ipv6-neighbors
<clear-subscriber-management-ipv6-neighbors>
clear system subscriber-management ipv6-neighbors address
<clear-subscriber-management-ipv6-neighbor-address>
clear system ipv6-neighbors interface
<clear-subscriber-management-ipv6-neighbor-interface>
clear system subscriber-management statistics
<clear-subscriber-management-statistics>
clear dot1x
<clear-dot1x>
clear dot1x eapol-block
<clear-dot1x-eapol-block>
clear dot1x eapol-block interface
<clear-dot1x-eapol-block-interface>
clear dot1x eapol-block mac-address
<clear-dot1x-eapol-block-mac-address>
clear dot1x firewall
<clear-dot1x-firewall>
clear dot1x firewall interface
<clear-dot1x-firewall-interface>
clear dot1x interface
<clear-dot1x-interface-session>
clear dot1x mac-address
<clear-dot1x-mac-session>
clear dot1x statistics
<clear-dot1x-statistics>
clear dot1x statistics interface
<clear-dot1x-statistics-interface>
clear error
clear error bpdu
<clear-bpdu-error>
clear error bpdu interface
<clear-bpdu-error-interface>
clear error loop-detect
<clear-loop-detect>
clear error loop-detect interface
<clear-loop-detect-error>
clear error mac-rewrite
<clear-mac-rewrite-error>
clear esis
clear esis adjacency
<clear-esis-adjacency>
clear esis statistics
<clear-esis-statistics>
clear ethernet-switching
clear ethernet-switching evpn
clear ethernet-switching evpn arp-table
<clear-ethernet-switching-evpn-arp-table>
clear ethernet-switching mac-learning-log
<clear-ethernet-switching-mac-learning-log>
clear ethernet-switching recovery-timeout
<clear-ethernet-switching-recovery>
clear ethernet-switching recovery-timeout interface
<clear-ethernet-switching-recovery-interface>
clear ethernet-switching satellite
clear ethernet-switching satellite logging
<clear-satellite-control-logging>
clear ethernet-switching satellite vlan-auto-sense
<clear-satellite-control-plane-vlan-auto-sense>
clear ethernet-switching table
<clear-ethernet-switching-table>
clear ethernet-switching table interface
<clear-ethernet-switching-interface-table>
clear ethernet-switching table persistent-learning
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning interface
<clear-ethernet-switching-table-persistent-learning>
clear ethernet-switching table persistent-learning mac
<clear-ethernet-switching-table-persistent-learning-mac>
clear evpn
clear evpn arp-table
<clear-evpn-arp-table>
clear evpn mac-table
<clear-evpn-mac-table>
clear evpn mac-table interface
<clear-evpn-interface-mac-table>
clear evpn nd-table
<clear-evpn-nd-table>
clear extensible-subscriber-services
clear extensible-subscriber-services counters
<clear-extensible-subscriber-services-counters>
clear extensible-subscriber-services sessions
<clear-extensible-subscriber-services-sessions>
clear fabric
<clear-fabric>
clear fabric statistics
<clear-fabric-statistics>
clear firewall
<clear-firewall-counters>
clear firewall all
<clear-all-firewall-conters>
clear firewall log
<clear-firewall-log>
clear firewall policer
clear firewall policer counter
clear firewall policer counter all
<clear-interface-aggregate-fwd-options>
<clear-interface-aggregate-fwd-options-all>
clear helper
clear helper statistics
<clear-helper-statistics-information>
clear igmp
clear igmp membership
<clear-igmp-membership>
clear igmp snooping
clear igmp snooping membership
<clear-igmp-snooping-membership>
clear igmp snooping membership bridge-domain
<clear-igmp-snooping-bridge-domain-membership>
clear igmp snooping membership vlan
<clear-igmp-snooping-vlan-membership>
clear igmp snooping statistics
<clear-igmp-snooping-statistics>
clear igmp snooping statistics bridge-domain
<clear-igmp-snooping-bridge-domain-statistics>
clear igmp snooping statistics vlan
<clear-igmp-snooping-vlan-statistics>
clear igmp statistics
<clear-igmp-statistics>
clear ike
<clear-ike-security-associations>
clear ike statistics
<clear-ike-statistics>
clear ilmi
<clear-ilmi-statistics>
clear interfaces
<clear-interfaces>
clear interfaces interface-set
<clear-interfaces-interface-set>
clear interfaces interface-set statistics
<clear-interfaces-interface-set-statistics>
clear interfaces interface-set statistics all
<clear-interfaces-interface-set-statistics-all>
clear interfaces interval
<clear-interfaces-interval>
clear interfaces mac-database
<clear-interfaces-mac-database>
clear interfaces mac-database statistics
<clear-interfaces-mac-database-statistics>
clear interfaces mac-database statistics all
<clear-interfaces-mac-database-statistics-all>
clear interfaces statistics
<clear-interfaces-statistics>
clear interfaces statistics all
<clear-interfaces-statistics-all>
clear interfaces transport
<clear-interfaces-transport-information>
clear interfaces transport optics
<clear-interface-transport-optics-information>
clear interfaces transport optics interval
<clear-interface-transport-optics-interval-information>
clear ipsec
<clear-ipsec-security-associations>
clear ipv6
<clear-ipv6-nd-information>
clear ipv6 neighbors all
<clear-ipv6-all-neighbors>
clear isis adjacency
<clear-isis-adjacency-information>
clear isis database
<clear-isis-database-information>
clear isis layer2-map
<clear-isis-layer2-map-information>
clear isis overload
<clear-isis-overload-information>
clear isis statistics
<clear-isis-statistics-information>
clear ipv6 router-advertisement
<clear-lacp>
clear lacp statistics
<clear-lacp-statistics>
clear 12-learning
<clear-12-learning-evpn>
clear 12-learning evpn arp-statistics
<clear-evpn-arp-statistics>
clear 12-learning evpn arp-statistics interface
<clear-evpn-arp-statistics-interface>
clear 12-learning evpn nd-statistics
<clear-evpn-nd-statistics>
clear 12-learning evpn nd-statistics interface
<clear-evpn-nd-statistics-interface>
clear 12-learning mac-move-buffer
<clear-12-learning-mac-move-buffer>
clear 12-learning mac-move-buffer active
<clear-12-learning-mac-move-buffer-active>
clear-12-learning-redundancy-group
<clear-12-learning-redundancy-group-statistics>
clear l2-learning remote-backbone-edge-bridges
<clear-l2-learning-remote-backbone-edge-bridges>
clear l2circuit
clear ldp
clear ldp statistics
<clear-ldp-statistics>
clear ldp statistics interface
<clear-ldp-interface-hello-statistics>
clear ldp neighbor
<clear-ldp-neighbors>
clear ldp session
<clear-ldp-sessions>
clear lldp
clear lldp neighbors
<clear-lldp-neighbors>
clear lldp neighbors interface
<clear-lldp-interface-neighbors>
clear lldp statistics
<clear-lldp-statistics>
clear lldp statistics interface
<clear-lldp-interface-statistics>
clear loop-detect
clear loop-detect statistics
clear loop-detect statistics interface
<clear-loop-detect-statistics-information>
clear mld
clear mld membership
<clear-mld-membership>
clear mld snooping
clear mld snooping membership
<clear-mld-snooping-membership>
clear mld snooping membership bridge-domain
<clear-mld-snooping-bridge-domain-membership>
clear mld snooping membership vlan
<clear-mld-snooping-vlan-membership>
clear mld snooping statistics
<clear-mld-snooping-statistics>
clear mld snooping statistics bridge-domain
<clear-mld-snooping-bridge-domain-statistics>
clear mld snooping statistics vlan
<clear-mld-snooping-vlan-statistics>
clear mld statistics
<clear-mld-statistics>
clear mobile-ip
clear mobile-ip binding
clear mobile-ip binding all
    <clear-binding-all>
clear mobile-ip binding ip-address
    <clear-binding-ip>
clear mobile-ip binding nai
    <clear-binding-nai>
clear mobile-ip visitor
clear mobile-ip visitor all
    <clear-visitor-all>
clear mobile-ip visitor ip-address
    <clear-visitor-ip>
clear mobile-ip visitor nai
    <clear-visitor-nai>
clear mpls
    clear mpls lsp
        <clear-mpls-lsp-information>
clear mpls static-lsp
        <clear-mpls-static-lsp-information>
clear mpls traceroute
clear mpls traceroute database
clear mpls traceroute database ldp
    <clear-mpls-traceroute-database-ldp>
clear msdp
clear msdp cache
    <clear-msdp-cache>
clear msdp statistics
    <clear-msdp-statistics>
clear multicast
clear multicast bandwidth-admission
    <clear-multicast-bandwidth-admission
clear multicast forwarding-cache
clear multicast scope
    <clear-multicast-scope-statistics>
clear multicast sessions
    <clear-multicast-sessions>
clear multicast statistics
    <clear-multicast-statistics>
clear mvrp
clear mvrp statistics
clear network-access
clear network-access aaa
clear network-access aaa statistics
  clear-aaa-statistics-table>
clear network-access aaa statistics address-assignment
clear network-access aaa statistics address-assignment client
  clear-aaa-address-assignment-client-statistics>
clear network-access aaa statistics address-assignment pool
  clear-aaa-address-assignment-pool-statistics>
clear network-access aaa subscriber
  clear-aaa-subscriber-table>
clear network-access aaa subscriber statistics
  clear-aaa-subscriber-table-specific-statistics>
clear network-access address-assignment
  clear-address-assignment-preserved>
clear network-access ocs
clear network-access ocs statistics
  clear-ocs-statistics-information>
clear network-access pcrf
clear network-access pcrf statistics
  clear-pcrf-statistics-information>
clear network-access pcrf subscribers
  clear-pcrf-subscribers>
clear network-access requests
clear network-access requests pending
  clear-authentication-pending-table>
clear network-access requests statistics
  clear-authentication-statistics>
clear network-access securid-node-secret-file
  clear-node-secret-file>
clear oam
clear oam ethernet
  clear oam ethernet connectivity-fault-management
  clear oam ethernet connectivity-fault-management continuity-measurement
  clear-cfm-continuity-measurement>
clear oam ethernet connectivity-fault-management delay-statistics
  clear-cfm-delay-statistics>
clear oam ethernet connectivity-fault-management event
  clear-cfm-action-profile-event>
clear oam ethernet connectivity-fault-management loss-statistics
<clear-cfm-loss-statistics>
clear oam ethernet connectivity-fault-management path-database
  <clear-cfm-linktrace-path-database>
clear oam ethernet connectivity-fault-management policer
  <clear-cfm-policer-statistics>
clear oam ethernet connectivity-fault-management sla-iterator-history
  <clear-cfm-iterator-history>
clear oam ethernet connectivity-fault-management sla-iterator-statistics
  <clear-cfm-iterator-statistics>
clear oam ethernet connectivity-fault-management statistics
  <clear-cfm-statistics>
clear oam ethernet connectivity-fault-management synthetic-loss-statistics
  <clear-cfm-slm-statistics>
clear oam ethernet link-fault-management
  <clear-lfmd-state>
clear oam ethernet link-fault-management state
    <clear-lfmd-state>
clear oam ethernet link-fault-management statistics
    <clear-lfmd-statistics>
clear oam ethernet link-fault-management statistics action-profile
    <clear-lfmd-action-profile-statistics>
clear oam ethernet lmi
  <clear-elmi-statistics>
clear ospf
  <clear-ospf-database-information>
clear ospf database
  <clear-ospf-database-protection>
clear ospf io-statistics
  <clear-ospf-io-statistics-information>
clear ospf neighbor
    <clear-ospf-neighbor-information>
clear ospf overload
  <clear-ospf-overload-information>
clear ospf statistics
  <clear-ospf-statistics-information>
clear ospf3
  <clear-ospf3-database-information>
clear ospf3 database
  <clear-ospf3-database-protection>
clear ospf3 database-protection
  <clear-ospf3-database-protection>
clear ospf3 io-statistics
<clear-ospf3-io-statistics-information>
clear ospf3 neighbor
<clear-ospf3-neighbor-information>
clear ospf3 overload
<clear-ospf3-overload-information>
clear ospf3 statistics
<clear-ospf3-io-statistics-information>
clear ovsdb
clear ovsdb commit
clear ovsdb commit failures
<clear-ovsdb-commit-failure-information>
clear ovsdb statistics
clear ovsdb statistics interface
clear ovsdb statistics interface all
<clear-ovsdb-interfaces-statistics-all>
clear performance-monitoring
clear performance-monitoring mpls
clear performance-monitoring mpls lsp
<clear-pm-mpls-lsp-information>
clear pfe
clear pfe statistics
clear pfe statistics fabric
clear pfe statistics traffic detail
clear pfe statistics traffic egress-queues fpc
clear pfe statistics traffic multicast
clear pfe statistics traffic multicast fpc
clear pfe tcam-errors
clear pfe tcam-errors all-tcam-stages
<clear-pfe-tcam-errors-all-tcam-stages>
clear pfe tcam-errors app
<clear-pfe-tcam-errors-app>
clear pfe tcam-errors app bd-dtag-validate
<clear-pfe-tcam-errors-app-bd-dtag-validate>
clear pfe tcam-errors app bd-dtag-validate detail
clear pfe tcam-errors app bd-dtag-validate list-related-apps
clear pfe tcam-errors app bd-dtag-validate list-shared-apps
clear pfe tcam-errors app bd-dtag-validate shared-usage
clear pfe tcam-errors app bd-dtag-validate shared-usage detail
clear pfe tcam-errors app bd-tpid-swap
<clear-pfe-tcam-errors-app-bd-tpid-swap>
clear pfe tcam-errors app bd-tpid-swap detail
clear pfe tcam-errors app bd-tpid-swap list-related-apps
clear pfe tcam-errors app bd-tpid-swap list-shared-apps
clear pfe tcam-errors app bd-tpid-swap shared-usage
clear pfe tcam-errors app bd-tpid-swap shared-usage detail
  <clear-pfe-tcam-errors-app-bd-tpid-swap>
clear pfe tcam-errors app cfm-bd-filter
  <clear-pfe-tcam-errors-app-cfm-bd-filter>
clear pfe tcam-errors app cfm-bd-filter detail
clear pfe tcam-errors app cfm-bd-filter list-related-apps
clear pfe tcam-errors app cfm-bd-filter list-shared-apps
clear pfe tcam-errors app cfm-bd-filter shared-usage
clear pfe tcam-errors app cfm-bd-filter shared-usage detail
clear pfe tcam-errors app cfm-filter
  <clear-pfe-tcam-errors-app-cfm-filter>
clear pfe tcam-errors app cfm-filter detail
clear pfe tcam-errors app cfm-filter list-related-apps
clear pfe tcam-errors app cfm-filter list-shared-apps
clear pfe tcam-errors app cfm-filter shared-usage
clear pfe tcam-errors app cfm-filter shared-usage detail
clear pfe tcam-errors app cfm-vpls-filter
  <clear-pfe-tcam-errors-app-cfm-vpls-filter>
clear pfe tcam-errors app cfm-vpls-filter detail
clear pfe tcam-errors app cfm-vpls-filter list-related-apps
clear pfe tcam-errors app cfm-vpls-filter list-shared-apps
clear pfe tcam-errors app cfm-vpls-filter shared-usage
clear pfe tcam-errors app cfm-vpls-filter shared-usage detail
clear pfe tcam-errors app cfm-vpls-ifl-filter
  <clear-pfe-tcam-errors-app-cfm-vpls-ifl-filter>
clear pfe tcam-errors app cfm-vpls-ifl-filter detail
clear pfe tcam-errors app cfm-vpls-ifl-filter list-related-apps
clear pfe tcam-errors app cfm-vpls-ifl-filter list-shared-apps
clear pfe tcam-errors app cfm-vpls-ifl-filter shared-usage
clear pfe tcam-errors app cfm-vpls-ifl-filter shared-usage detail
clear pfe tcam-errors app cos-fc
  <clear-pfe-tcam-errors-app-cos-fc>
clear pfe tcam-errors app cos-fc detail
clear pfe tcam-errors app cos-fc list-related-apps
clear pfe tcam-errors app cos-fc list-shared-apps
clear pfe tcam-errors app cos-fc shared-usage
clear pfe tcam-errors app cos-fc shared-usage detail
clear pfe tcam-errors app fw-ccc-in
  <clear-pfe-tcam-errors-app-fw-ccc-in>
clear pfe tcam-errors app fw-ccc-in detail
clear pfe tcam-errors app fw-ccc-in list-related-apps
clear pfe tcam-errors app fw-ccc-in list-shared-apps
clear pfe tcam-errors app fw-ccc-in shared-usage
clear pfe tcam-errors app fw-ccc-in shared-usage detail
clear pfe tcam-errors app fw-family-out
<clear-pfe-tcam-errors-app-fw-family-out>
clear pfe tcam-errors app fw-family-out detail
clear pfe tcam-errors app fw-family-out list-related-apps
clear pfe tcam-errors app fw-family-out list-shared-apps
clear pfe tcam-errors app fw-family-out shared-usage
clear pfe tcam-errors app fw-family-out shared-usage detail
clear pfe tcam-errors app fw-fbf
<clear-pfe-tcam-errors-app-fw-fbf>
clear pfe tcam-errors app fw-fbf detail
clear pfe tcam-errors app fw-fbf list-related-apps
clear pfe tcam-errors app fw-fbf list-shared-apps
clear pfe tcam-errors app fw-fbf shared-usage
clear pfe tcam-errors app fw-fbf shared-usage detail
clear pfe tcam-errors app fw-fbf-inet6
<clear-pfe-tcam-errors-app-fw-fbf-inet6>
clear pfe tcam-errors app fw-fbf-inet6 detail
clear pfe tcam-errors app fw-fbf-inet6 list-related-apps
clear pfe tcam-errors app fw-fbf-inet6 list-shared-apps
clear pfe tcam-errors app fw-fbf-inet6 shared-usage
clear pfe tcam-errors app fw-fbf-inet6 shared-usage detail
clear pfe tcam-errors app fw-ifl-in
<clear-pfe-tcam-errors-app-fw-ifl-in>
clear pfe tcam-errors app fw-ifl-in detail
clear pfe tcam-errors app fw-ifl-in list-related-apps
clear pfe tcam-errors app fw-ifl-in list-shared-apps
clear pfe tcam-errors app fw-ifl-in shared-usage
clear pfe tcam-errors app fw-ifl-in shared-usage detail
clear pfe tcam-errors app fw-ifl-out
<clear-pfe-tcam-errors-app-fw-ifl-out>
clear pfe tcam-errors app fw-ifl-out detail
clear pfe tcam-errors app fw-ifl-out list-related-apps
clear pfe tcam-errors app fw-ifl-out list-shared-apps
clear pfe tcam-errors app fw-ifl-out shared-usage
clear pfe tcam-errors app fw-ifl-out shared-usage detail
clear pfe tcam-errors app fw-inet-ftf
<clear-pfe-tcam-errors-app-fw-inet-ftf>
clear pfe tcam-errors app fw-inet-ftf detail
clear pfe tcam-errors app fw-inet-ftf list-related-apps
clear pfe tcam-errors app fw-inet-ftf list-shared-apps
clear pfe tcam-errors app fw-inet-ftf shared-usage
clear pfe tcam-errors app fw-inet-ftf shared-usage detail
clear pfe tcam-errors app fw-inet-in
<clear-pfe-tcam-errors-app-fw-inet-in>
clear pfe tcam-errors app fw-inet-in detail
clear pfe tcam-errors app fw-inet-in list-related-apps
clear pfe tcam-errors app fw-inet-in list-shared-apps
clear pfe tcam-errors app fw-inet-in shared-usage
clear pfe tcam-errors app fw-inet-in shared-usage detail
clear pfe tcam-errors app fw-inet-pm
<clear-pfe-tcam-errors-app-fw-inet-pm>
clear pfe tcam-errors app fw-inet-pm detail
clear pfe tcam-errors app fw-inet-pm list-related-apps
clear pfe tcam-errors app fw-inet-pm list-shared-apps
clear pfe tcam-errors app fw-inet-pm shared-usage
clear pfe tcam-errors app fw-inet-pm shared-usage detail
clear pfe tcam-errors app fw-inet-rpf
<clear-pfe-tcam-errors-app-fw-inet-rpf>
clear pfe tcam-errors app fw-inet-rpf detail
clear pfe tcam-errors app fw-inet-rpf list-related-apps
clear pfe tcam-errors app fw-inet-rpf list-shared-apps
clear pfe tcam-errors app fw-inet-rpf shared-usage
clear pfe tcam-errors app fw-inet-rpf shared-usage detail
clear pfe tcam-errors app fw-inet-rpf
<clear-pfe-tcam-errors-app-fw-inet-rpf>
clear pfe tcam-errors app fw-inet-rpf detail
clear pfe tcam-errors app fw-inet-rpf list-related-apps
clear pfe tcam-errors app fw-inet-rpf list-shared-apps
clear pfe tcam-errors app fw-inet-rpf shared-usage
clear pfe tcam-errors app fw-inet-rpf shared-usage detail
clear pfe tcam-errors app fw-inet6-family-out
<clear-pfe-tcam-errors-app-fw-inet6-family-out>
clear pfe tcam-errors app fw-inet6-family-out detail
clear pfe tcam-errors app fw-inet6-family-out list-related-apps
clear pfe tcam-errors app fw-inet6-family-out list-shared-apps
clear pfe tcam-errors app fw-inet6-family-out shared-usage
clear pfe tcam-errors app fw-inet6-family-out shared-usage detail
clear pfe tcam-errors app fw-inet6-ftf
<clear-pfe-tcam-errors-app-fw-inet6-ftf>
clear pfe tcam-errors app fw-inet6-ftf detail
clear pfe tcam-errors app fw-inet6-ftf list-related-apps
clear pfe tcam-errors app fw-inet6-ff list-shared-apps
clear pfe tcam-errors app fw-inet6-ff shared-usage
clear pfe tcam-errors app fw-inet6-ff shared-usage detail
clear pfe tcam-errors app fw-inet6-in
<clear-pfe-tcam-errors-app-fw-inet6-in>
clear pfe tcam-errors app fw-inet6-in detail
clear pfe tcam-errors app fw-inet6-in list-related-apps
clear pfe tcam-errors app fw-inet6-in list-shared-apps
clear pfe tcam-errors app fw-inet6-in shared-usage
clear pfe tcam-errors app fw-inet6-in shared-usage detail
clear pfe tcam-errors app fw-inet6-rpf
<clear-pfe-tcam-errors-app-fw-inet6-rpf>
clear pfe tcam-errors app fw-inet6-rpf detail
clear pfe tcam-errors app fw-inet6-rpf list-related-apps
clear pfe tcam-errors app fw-inet6-rpf list-shared-apps
clear pfe tcam-errors app fw-inet6-rpf shared-usage
clear pfe tcam-errors app fw-inet6-rpf shared-usage detail
clear pfe tcam-errors app fw-12-in
<clear-pfe-tcam-errors-app-fw-12-in>
clear pfe tcam-errors app fw-12-in detail
clear pfe tcam-errors app fw-12-in list-related-apps
clear pfe tcam-errors app fw-12-in list-shared-apps
clear pfe tcam-errors app fw-12-in shared-usage
clear pfe tcam-errors app fw-12-in shared-usage detail
clear pfe tcam-errors app fw-mpls-in
<clear-pfe-tcam-errors-app-fw-mpls-in>
clear pfe tcam-errors app fw-mpls-in detail
clear pfe tcam-errors app fw-mpls-in list-related-apps
clear pfe tcam-errors app fw-mpls-in list-shared-apps
clear pfe tcam-errors app fw-mpls-in shared-usage
clear pfe tcam-errors app fw-mpls-in shared-usage detail
clear pfe tcam-errors app fw-semantics
<clear-pfe-tcam-errors-app-fw-semantics>
clear pfe tcam-errors app fw-semantics detail
clear pfe tcam-errors app fw-semantics list-related-apps
clear pfe tcam-errors app fw-semantics list-shared-apps
clear pfe tcam-errors app fw-semantics shared-usage
clear pfe tcam-errors app fw-semantics shared-usage detail
clear pfe tcam-errors app fw-vpls-in
<clear-pfe-tcam-errors-app-fw-vpls-in>
clear pfe tcam-errors app fw-vpls-in detail
clear pfe tcam-errors app fw-vpls-in list-related-apps
clear pfe tcam-errors app fw-vpls-in list-shared-apps
clear pfe tcam-errors app fw-vpls-in shared-usage
clear pfe tcam-errors app fw-vpls-in shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-eqr
<clear-pfe-tcam-errors-app-gr-ifl-statistics-eqr>
clear pfe tcam-errors app gr-ifl-stats-eqr detail
clear pfe tcam-errors app gr-ifl-stats-eqr list-related-apps
clear pfe tcam-errors app gr-ifl-stats-eqr list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-eqr shared-usage
clear pfe tcam-errors app gr-ifl-stats-eqr shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-ing
<clear-pfe-tcam-errors-app-gr-ifl-statistics-ing>
clear pfe tcam-errors app gr-ifl-stats-ing detail
clear pfe tcam-errors app gr-ifl-stats-ing list-related-apps
clear pfe tcam-errors app gr-ifl-stats-ing list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-ing shared-usage
clear pfe tcam-errors app gr-ifl-stats-ing shared-usage detail
clear pfe tcam-errors app gr-ifl-stats-preing
<clear-pfe-tcam-errors-app-gr-ifl-statistics-preing>
clear pfe tcam-errors app gr-ifl-stats-preing detail
clear pfe tcam-errors app gr-ifl-stats-preing list-related-apps
clear pfe tcam-errors app gr-ifl-stats-preing list-shared-apps
clear pfe tcam-errors app gr-ifl-stats-preing shared-usage
clear pfe tcam-errors app gr-ifl-stats-preing shared-usage detail
< clear pfe tcam-errors app ifd-src-mac-fil
<clear-pfe-tcam-errors-app-ifd-src-mac-fil>
clear pfe tcam-errors app ifd-src-mac-fil detail
clear pfe tcam-errors app ifd-src-mac-fil list-related-apps
clear pfe tcam-errors app ifd-src-mac-fil list-shared-apps
clear pfe tcam-errors app ifd-src-mac-fil shared-usage
clear pfe tcam-errors app ifd-src-mac-fil shared-usage detail
clear pfe tcam-errors app ifl-statistics-in
<clear-pfe-tcam-errors-app-ifl-statistics-in>
clear pfe tcam-errors app ifl-statistics-in detail
clear pfe tcam-errors app ifl-statistics-in list-related-apps
clear pfe tcam-errors app ifl-statistics-in list-shared-apps
clear pfe tcam-errors app ifl-statistics-in shared-usage
clear pfe tcam-errors app ifl-statistics-in shared-usage detail
clear pfe tcam-errors app ifl-statistics-out
<clear-pfe-tcam-errors-app-ifl-statistics-out>
clear pfe tcam-errors app ifl-statistics-out detail
clear pfe tcam-errors app ifl-statistics-out list-related-apps
clear pfe tcam-errors app ifl-statistics-out list-shared-apps
clear pfe tcam-errors app ifl-statistics-out shared-usage
clear pfe tcam-errors app ifl-statistics-out shared-usage detail
clear pfe tcam-errors app ing-out-iff
<clear-pfe-tcam-errors-app-ing-out-iff>
clear pfe tcam-errors app ing-out-iff detail
clear pfe tcam-errors app ing-out-iff list-related-apps
clear pfe tcam-errors app ing-out-iff list-shared-apps
clear pfe tcam-errors app ing-out-iff shared-usage
clear pfe tcam-errors app ing-out-iff shared-usage detail
clear pfe tcam-errors app ip-mac-val
<clear-pfe-tcam-errors-app-ip-mac-val>
clear pfe tcam-errors app ip-mac-val detail
clear pfe tcam-errors app ip-mac-val list-related-apps
clear pfe tcam-errors app ip-mac-val list-shared-apps
clear pfe tcam-errors app ip-mac-val shared-usage
clear pfe tcam-errors app ip-mac-val shared-usage detail
clear pfe tcam-errors app ip-mac-val-bcast
<clear-pfe-tcam-errors-app-ip-mac-val-bcast>
clear pfe tcam-errors app ip-mac-val-bcast detail
clear pfe tcam-errors app ip-mac-val-bcast list-related-apps
clear pfe tcam-errors app ip-mac-val-bcast list-shared-apps
clear pfe tcam-errors app ip-mac-val-bcast shared-usage
clear pfe tcam-errors app ip-mac-val-bcast shared-usage detail
clear pfe tcam-errors app ipsec-reverse-fil
<clear-pfe-tcam-errors-app-ipsec-reverse-fil>
clear pfe tcam-errors app ipsec-reverse-fil detail
clear pfe tcam-errors app ipsec-reverse-fil list-related-apps
clear pfe tcam-errors app ipsec-reverse-fil list-shared-apps
clear pfe tcam-errors app ipsec-reverse-fil shared-usage
clear pfe tcam-errors app ipsec-reverse-fil shared-usage detail
clear pfe tcam-errors app irb-cos-rw
<clear-pfe-tcam-errors-app-irb-cos-rw>
clear pfe tcam-errors app irb-cos-rw detail
clear pfe tcam-errors app irb-cos-rw list-related-apps
clear pfe tcam-errors app irb-cos-rw list-shared-apps
clear pfe tcam-errors app irb-cos-rw shared-usage
clear pfe tcam-errors app irb-cos-rw shared-usage detail
clear pfe tcam-errors app irb-fixed-cos
<clear-pfe-tcam-errors-app-irb-fixed-cos>
clear pfe tcam-errors app irb-fixed-cos detail
clear pfe tcam-errors app irb-fixed-cos list-related-apps
clear pfe tcam-errors app irb-fixed-cos list-shared-apps
clear pfe tcam-errors app irb-fixed-cos shared-usage
clear pfe tcam-errors app irb-fixed-cos shared-usage detail
clear pfe tcam-errors app irb-inet6-fil
<clear-pfe-tcam-errors-app-irb-inet6-fil>
clear pfe tcam-errors app irb-inet6-fil detail
clear pfe tcam-errors app irb-inet6-fil list-related-apps
clear pfe tcam-errors app irb-inet6-fil list-shared-apps
clear pfe tcam-errors app irb-inet6-fil shared-usage
clear pfe tcam-errors app irb-inet6-fil shared-usage detail
clear pfe tcam-errors app lfm-802.3ah-in
<clear-pfe-tcam-errors-app-lfm-802.3ah-in>
clear pfe tcam-errors app lfm-802.3ah-in detail
clear pfe tcam-errors app lfm-802.3ah-in list-related-apps
clear pfe tcam-errors app lfm-802.3ah-in list-shared-apps
clear pfe tcam-errors app lfm-802.3ah-in shared-usage
clear pfe tcam-errors app lfm-802.3ah-in shared-usage detail
clear pfe tcam-errors app lfm-802.3ah-out
<clear-pfe-tcam-errors-app-lfm-802.3ah-out>
clear pfe tcam-errors app lfm-802.3ah-out detail
clear pfe tcam-errors app lfm-802.3ah-out list-related-apps
clear pfe tcam-errors app lfm-802.3ah-out list-shared-apps
clear pfe tcam-errors app lfm-802.3ah-out shared-usage
clear pfe tcam-errors app lfm-802.3ah-out shared-usage detail
clear pfe tcam-errors app lo0-inet-fil
<clear-pfe-tcam-errors-app-lo0-inet-fil>
clear pfe tcam-errors app lo0-inet-fil detail
clear pfe tcam-errors app lo0-inet-fil list-related-apps
clear pfe tcam-errors app lo0-inet-fil list-shared-apps
clear pfe tcam-errors app lo0-inet-fil shared-usage
clear pfe tcam-errors app lo0-inet-fil shared-usage detail
clear pfe tcam-errors app lo0-inet6-fil
<clear-pfe-tcam-errors-app-lo0-inet6-fil>
clear pfe tcam-errors app lo0-inet6-fil detail
clear pfe tcam-errors app lo0-inet6-fil list-related-apps
clear pfe tcam-errors app lo0-inet6-fil list-shared-apps
clear pfe tcam-errors app lo0-inet6-fil shared-usage
clear pfe tcam-errors app lo0-inet6-fil shared-usage detail
clear pfe tcam-errors app mac-drop-cnt
<clear-pfe-tcam-errors-app-mac-drop-cnt>
clear pfe tcam-errors app mac-drop-cnt detail
clear pfe tcam-errors app mac-drop-cnt list-related-apps
clear pfe tcam-errors app mac-drop-cnt list-shared-apps
clear pfe tcam-errors app mac-drop-cnt shared-usage
clear pfe tcam-errors app mac-drop-cnt shared-usage detail
clear pfe tcam-errors app mrouter-port-in
<clear-pfe-tcam-errors-app-mrouter-port-in>
clear pfe tcam-errors app mrouter-port-in detail
clear pfe tcam-errors app mrouter-port-in list-related-apps
clear pfe tcam-errors app mrouter-port-in list-shared-apps
clear pfe tcam-errors app mrouter-port-in shared-usage
clear pfe tcam-errors app mrouter-port-in shared-usage detail
clear pfe tcam-errors app napt-reverse-fil
<clear-pfe-tcam-errors-app-napt-reverse-fil>
clear pfe tcam-errors app napt-reverse-fil detail
clear pfe tcam-errors app napt-reverse-fil list-related-apps
clear pfe tcam-errors app napt-reverse-fil list-shared-apps
clear pfe tcam-errors app napt-reverse-fil shared-usage
clear pfe tcam-errors app napt-reverse-fil shared-usage detail
clear pfe tcam-errors app no-local-switching
<clear-pfe-tcam-errors-app-no-local-switching>
clear pfe tcam-errors app no-local-switching detail
clear pfe tcam-errors app no-local-switching list-related-apps
clear pfe tcam-errors app no-local-switching list-shared-apps
clear pfe tcam-errors app no-local-switching shared-usage
clear pfe tcam-errors app no-local-switching shared-usage detail
clear pfe tcam-errors app ptpoe-cos-rw
<clear-pfe-tcam-errors-app-ptpoe-cos-rw>
clear pfe tcam-errors app ptpoe-cos-rw detail
clear pfe tcam-errors app ptpoe-cos-rw list-related-apps
clear pfe tcam-errors app ptpoe-cos-rw list-shared-apps
clear pfe tcam-errors app ptpoe-cos-rw shared-usage
clear pfe tcam-errors app ptpoe-cos-rw shared-usage detail
clear pfe tcam-errors app rfc2544-layer2-in
<clear-pfe-tcam-errors-app-rfc2544-layer2-in>
clear pfe tcam-errors app rfc2544-layer2-in detail
clear pfe tcam-errors app rfc2544-layer2-in list-related-apps
clear pfe tcam-errors app rfc2544-layer2-in list-shared-apps
clear pfe tcam-errors app rfc2544-layer2-in shared-usage
clear pfe tcam-errors app rfc2544-layer2-in shared-usage detail
clear pfe tcam-errors app rfc2544-layer2-out
<clear-pfe-tcam-errors-app-rfc2544-layer2-out>
clear pfe tcam-errors app rfc2544-layer2-out detail
clear pfe tcam-errors app rfc2544-layer2-out list-related-apps
clear pfe tcam-errors app rfc2544-layer2-out list-shared-apps
clear pfe tcam-errors app rfc2544-layer2-out shared-usage
clear pfe tcam-errors app rfc2544-layer2-out shared-usage detail
clear pfe tcam-errors app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
clear pfe tcam-errors app vpls-mesh-group-mcast detail
clear pfe tcam-errors app vpls-mesh-group-mcast list-related-apps
clear pfe tcam-errors app vpls-mesh-group-mcast list-shared-apps
clear pfe tcam-errors app vpls-mesh-group-mcast shared-usage
clear pfe tcam-errors app vpls-mesh-group-mcast shared-usage detail
clear pfe tcam-errors app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
clear pfe tcam-errors app vpls-mesh-group-ucast detail
clear pfe tcam-errors app vpls-mesh-group-ucast list-related-apps
clear pfe tcam-errors app vpls-mesh-group-ucast list-shared-apps
clear pfe tcam-errors app vpls-mesh-group-ucast shared-usage
clear pfe tcam-errors app vpls-mesh-group-ucast shared-usage detail
clear pfe tcam-errors tcam-stage
clear pfe tcam-errors tcam-stage egress
<clear-pfe-tcam-errors-egress-tcam-stage>
clear pfe tcam-errors tcam-stage egress app
clear-pfe-tcam-errors-egress-app
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate
<clear-pfe-tcam-errors-egress-app-bd-dtag-validate>
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate detail
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate list-related-apps
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate list-shared-apps
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate shared-usage
clear pfe tcam-errors tcam-stage egress app bd-dtag-validate shared-usage detail
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap
<clear-pfe-tcam-errors-egress-app-bd-tpid-swap>
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap detail
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap list-related-apps
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap list-shared-apps
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap shared-usage
clear pfe tcam-errors tcam-stage egress app bd-tpid-swap shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-family-out
<clear-pfe-tcam-errors-egress-app-fw-family-out>
clear pfe tcam-errors tcam-stage egress app fw-family-out detail
clear pfe tcam-errors tcam-stage egress app fw-family-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-family-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-family-out shared-usage
clear pfe tcam-errors tcam-stage egress app fw-family-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-ifl-out
<clear-pfe-tcam-errors-egress-app-fw-ifl-out>
clear pfe tcam-errors tcam-stage egress app fw-ifl-out detail
clear pfe tcam-errors tcam-stage egress app fw-ifl-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-ifl-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-ifl-out shared-usage
clear pfe tcam-errors tcam-stage egress app fw-ifl-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out
<clear-pfe-tcam-errors-egress-app-fw-inet6-family-out>
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out detail
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out list-related-apps
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out shared-usage
clear pfe tcam-errors tcam-stage egress app fw-inet6-family-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out
<clear-pfe-tcam-errors-egress-app-ifl-statistics-out>
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out detail
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out list-related-apps
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out shared-usage
clear pfe tcam-errors tcam-stage egress app ifl-statistics-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app irb-cos-rw
<clear-pfe-tcam-errors-egress-app-irb-cos-rw>
clear pfe tcam-errors tcam-stage egress app irb-cos-rw detail
clear pfe tcam-errors tcam-stage egress app irb-cos-rw list-related-apps
clear pfe tcam-errors tcam-stage egress app irb-cos-rw list-shared-apps
clear pfe tcam-errors tcam-stage egress app irb-cos-rw shared-usage
clear pfe tcam-errors tcam-stage egress app irb-cos-rw shared-usage detail
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out
<clear-pfe-tcam-errors-egress-app-lfm-802.3ah-out>
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out detail
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out list-related-apps
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage detail
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage
clear pfe tcam-errors tcam-stage egress app lfm-802.3ah-out shared-usage
detail
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw
<clear-pfe-tcam-errors-egress-app-ptpoe-cos-rw>
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw list-related-apps
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw list-shared-apps
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw shared-usage
clear pfe tcam-errors tcam-stage egress app ptpoe-cos-rw shared-usage
detail
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out
<clear-pfe-tcam-errors-egress-app-rfc2544-layer2-out>
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out
detail
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out
list-related-apps
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out list-shared-apps
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out shared-usage
clear pfe tcam-errors tcam-stage egress app rfc2544-layer2-out shared-usage
detail
clear pfe tcam-errors tcam-stage ingress
<clear-pfe-tcam-errors-ingress-tcam-stage>
clear pfe tcam-errors tcam-stage ingress app
<clear-pfe-tcam-errors-ingress-app>
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter
<clear-pfe-tcam-errors-ingress-app-cfm-bd-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter
detail
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-bd-filter shared-usage
detail
clear pfe tcam-errors tcam-stage ingress app cfm-filter
<clear-pfe-tcam-errors-ingress-app-cfm-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-filter
detail
clear pfe tcam-errors tcam-stage ingress app cfm-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app cfm-filter shared-usage
clear pfe tcam-errors tcam-stage ingress app cfm-filter shared-usage
detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter
<clear-pfe-tcam-errors-ingress-app-cfm-vpls-filter>
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter
detail
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter list-related-apps
clear pfe tcam-errors tcam-stage ingress app cfm-vpls-filter list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-pm shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-inet-rpf>
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet-rpf shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-inet6-ftf>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-ftf shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-inet6-in>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-in shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-inet6-rpf>
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf detail
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-inet6-rpf shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-l2-in>
clear pfe tcam-errors tcam-stage ingress app fw-l2-in detail
clear pfe tcam-errors tcam-stage ingress app fw-l2-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-l2-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-l2-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-l2-in shared-usage detail
<clear-pfe-tcam-errors-ingress-app-fw-mpls-in>
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in detail
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-mpls-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in detail
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in shared-usage
clear pfe tcam-errors tcam-stage ingress app fw-vpls-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-egr shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-ing shared-usage detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing detail
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing list-related-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing list-shared-apps
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing shared-usage
clear pfe tcam-errors tcam-stage ingress app gr-ifl-stats-preing shared-usage detail
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in detail
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in shared-usage
clear pfe tcam-errors tcam-stage ingress app ifl-statistics-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil
<clear-pfe-tcam-errors-ingress-app-ipsec-reverse-fil>
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil detail
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app ipsec-reverse-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos
<clear-pfe-tcam-errors-ingress-app-irb-fixed-cos>
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos detail
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos list-related-apps
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos list-shared-apps
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos shared-usage
clear pfe tcam-errors tcam-stage ingress app irb-fixed-cos shared-usage detail
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil
<clear-pfe-tcam-errors-ingress-app-irb-inet6-fil>
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil detail
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app irb-inet6-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in
<clear-pfe-tcam-errors-ingress-app-lfm-802.3ah-in>
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in detail
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in shared-usage
clear pfe tcam-errors tcam-stage ingress app lfm-802.3ah-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil
<clear-pfe-tcam-errors-ingress-app-lo0-inet-fil>
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app lo0-inet-fil shared-usage detail
<clear-pfe-tcam-errors-ingress-app-lo0-inet6-fil>
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil detail
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app lo0-inet6-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt
<clear-pfe-tcam-errors-ingress-app-mac-drop-cnt>
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt detail
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt list-related-apps
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt list-shared-apps
clear pfe tcam-errors tcam-stage ingress app mac-drop-cnt shared-usage
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in
<clear-pfe-tcam-errors-ingress-app-mrouter-port-in>
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in detail
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in list-related-apps
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in list-shared-apps
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in shared-usage
clear pfe tcam-errors tcam-stage ingress app mrouter-port-in shared-usage detail
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil
<clear-pfe-tcam-errors-ingress-app-napt-reverse-fil>
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil detail
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil list-related-apps
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil list-shared-apps
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil shared-usage
clear pfe tcam-errors tcam-stage ingress app napt-reverse-fil shared-usage detail
clear pfe tcam-errors tcam-stage ingress app no-local-switching
<clear-pfe-tcam-errors-ingress-app-no-local-switching>
clear pfe tcam-errors tcam-stage ingress app no-local-switching detail
clear pfe tcam-errors tcam-stage ingress app no-local-switching list-related-apps
clear pfe tcam-errors tcam-stage ingress app no-local-switching list-shared-apps
clear pfe tcam-errors tcam-stage ingress app no-local-switching shared-usage
clear pfe tcam-errors tcam-stage ingress app no-local-switching shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress
<clear-pfe-tcam-errors-pre-ingress-tcam-stage>
clear pfe tcam-errors tcam-stage pre-ingress app
<clear-pfe-tcam-errors-pre-ingress-app>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc detail
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc-detail>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc list-related-apps
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc-list-related-apps>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc list-shared-apps
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc-list-shared-apps>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc shared-usage
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc-shared-usage>
clear pfe tcam-errors tcam-stage pre-ingress app cos-fc shared-usage detail
<clear-pfe-tcam-errors-pre-ingress-app-cos-fc-shared-usage-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf list-related-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-list-related-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf list-shared-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-list-shared-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf shared-usage
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-shared-usage>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf shared-usage detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-shared-usage-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 list-related-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6-list-related-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 list-shared-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6-list-shared-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 shared-usage
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6-shared-usage>
clear pfe tcam-errors tcam-stage pre-ingress app fw-fbf-inet6 shared-usage detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-fbf-inet6-shared-usage-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics-detail>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics list-related-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics-list-related-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics list-shared-apps
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics-list-shared-apps>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics shared-usage
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics-shared-usage>
clear pfe tcam-errors tcam-stage pre-ingress app fw-semantics shared-usage detail
<clear-pfe-tcam-errors-pre-ingress-app-fw-semantics-shared-usage-detail>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil detail
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil-detail>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil list-related-apps
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil-list-related-apps>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil list-shared-apps
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil-list-shared-apps>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil shared-usage
<clear-pfe-tcam-errors-pre-ingress-app-ifd-src-mac-fil-shared-usage>
clear pfe tcam-errors tcam-stage pre-ingress app ifd-src-mac-fil shared-usage
detail
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff
<clear-pfe-tcam-errors-pre-ingress-app-ing-out-iff>
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff detail
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ing-out-iff shared-usage
detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val
<clear-pfe-tcam-errors-pre-ingress-app-ip-mac-val>
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val shared-usage
detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast
<clear-pfe-tcam-errors-pre-ingress-app-ip-mac-val-bcast>
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast detail
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app ip-mac-val-bcast shared-usage
detail
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in
<clear-pfe-tcam-errors-pre-ingress-app-rfc2544-layer2-in>
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in detail
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app rfc2544-layer2-in shared-usage
detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
shared-usage detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast detail
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-mcast
list-related-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage
clear pfe tcam-errors tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage detail
clear passive-monitoring
  <clear-passive-monitoring>
clear passive-monitoring statistics
  <clear-passive-monitoring-statistics>
clear pgm
clear pgm negative-acknowledgments
  <clear-pgm-negative-acknowledgments>
clear pgm source-path-messages
  <clear-pgm-source-path-messages>
clear pgm statistics
  <clear-pgm-statistics>
clear pim
clear pim join
  <clear-pim-join-state>
clear pim join-distribution
  <clear-pim-join-distribution>
clear pim register
  <clear-pim-register-state>
clear pim snooping
clear pim snooping join
clear pim snooping statistics
clear pim statistics
  <clear-pim-statistics>
clear poe
clear poe telemetries
clear poe telemetries interface
<clear-poe-telemetries-information>
clear ppp
clear ppp statistics
<clear-ppp-statistics-information>
clear pppoe
clear pppoe lockout
<clear-pppoe-lockout-timers>
clear pppoe lockout atm-identifier
<clear-pppoe-lockout-timers-atm>
clear pppoe lockout vlan-identifier
clear pppoe sessions
<clear-pppoe-sessions-information>
clear-pppoe-lockout-timers-vlan
clear pppoe statistics
<clear-pppoe-statistics-information>
clear pppoe statistics interfaces
<clear-pppoe-statistics-interface-information>
clear protection-group
<clear protection-group>
clear protection-group ethernet-ring
<clear-ethernet-ring-information>
clear protection-group ethernet-ring statistics
<clear-ethernet-ring-information>
clear r2cp
clear r2cp radio
<clear-r2cp-radio>
clear r2cp session
<clear-r2cp-session>
clear r2cp statistics
<clear-r2cp-statistics>
clear r2cp statistics radio
clear r2cp statistics session
clear rip
clear rip general-statistics
<clear-rip-general-statistics>
clear rip statistics
<clear-rip-statistics>
clear rip statistics peer
<clear-rip-peer-statistics>
clear ripng
clear ripng general-statistics
<clear-ripng-general-statistic>
clear ripng statistics
<clear-ripng-statistics>
clear rsvp
<clear-rsvp-session-information>
clear rsvp statistics
<clear-rsvp-counters-information>
clear security group-vpn
<clear-gvpn-group-information>
clear security group-vpn member ike
<clear-gvpn-ike-security-association>
clear security group-vpn member ipsec
<clear-gvpn-ipsec-security-association>
clear security group-vpn member ipsec security-associations statistics
<clear-gvpn-ipsec-security-association-statistics>
clear security group-vpn member ipsec statistics
<clear-gvpn-ipsec-statistics>
clear services
<clear-services-accounting-inline-jflow-flows>
clear services alg
<clear-appid-application-system-cache>
clear services alg statistics
<clear-appid-counter>
clear services application-aware-access-list
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics interface
<clear-application-aware-access-list-statistics-interface>
clear services application-aware-access-list statistics subscriber
<clear-application-aware-access-list-statistics-subscriber>
clear services application-identification
<clear-appid-application-system-cache>
clear services application-identification counter
<clear-appid-counter>
clear services application-identification counter ssl-encrypted-sessions
clear services application-identification statistics
<clear-appid-application-statistics>
clear services application-identification statistics cumulative
<clear-appid-application-statistics-cumulative>
clear services application-identification statistics interval
<clear-appid-application-statistics-interval>
clear services border-signaling-gateway
<clear-service-bsg-denied-messages>
clear services border-signaling-gateway name-resolution-cache
<clear-service-border-signaling-gateway-name-resolution-cache>
clear services border-signaling-gateway name-resolution-cache all
<clear-service-border-signaling-gateway-name-resolution-cache-all>
clear services border-signaling-gateway name-resolution-cache by-fqdn
<clear-border-signaling-gateway-name-resolution-cache-by-fqdn>
clear services border-signaling-gateway statistics
<clear-service-border-signaling-gateway-statistics>
clear services captive-portal-content-delivery
<clear-services-captive-portal-content-delivery>
clear services captive-portal-content-delivery statistics
<clear-cpcdd-interface-statistics>
clear services cos
<clear-services-cos-statistics>
clear services crtp
<clear-services-crtp-statistics>
clear services dynamic-flow-capture
<clear-services-dynamic-flow-capture>
clear services dynamic-flow-capture criteria
<clear-services-dynamic-flow-capture-criteria>
clear services dynamic-flow-capture sequence-number
<clear-services-dynamic-flow-capture-sequence-number>
clear services flow-collector
<clear-services-flow-collector-information>
clear services flow-collector statistics
<clear-services-flow-collector-statistics>
clear-service-msp-flow-ipaction-table
<clear-service-msp-flow-ipaction-table>
clear services ha
<clear-service-ha-statistics-information>
clear services hcm
<clear-services-hcm-pic-statistics>
clear services hcm statistics
<clear-services-hcm-statistics>
clear services ids
<clear-services-ids-tables>
clear services ids destination-table
<clear-services-ids-destination-table>
clear services ids pair-table
<clear-services-ids-pair-table>
clear services ids source-table
<clear-services-ids-source-table>
clear services inline
clear services inline nat
clear services inline nat pool
<clear-inline-nat-pool-information>
clear services inline nat statistics
<clear-inline-nat-statistics>
clear services inline softwire
clear services inline softwire statistics
<clear-inline-softwire-statistics>
clear services ipsec-vpn
clear services ipsec-vpn ipsec
<clear-services-ipsec-vpn-security-associations>
clear services ipsec-vpn ike
clear services ipsec-vpn ike security-associations
<clear-services-ike-security-associations>
clear services ipsec-vpn ike statistics
<clear-services-ike-statistics>
clear services pcp
clear services pcp epoch
<clear-services-pcp-statistics>
clear services pcp destination
<clear-services-pcp-destinations-information>
clear services 12tp
<clear-12tp-destinations-information>
clear services 12tp disconnect-cause-summary
<clear-12tp-disconnect-cause-summary>
clear services 12tp multilink
<clear-12tp-multilink-information>
clear services 12tp session
<clear-12tp-session-information>
clear services 12tp destination
clear services 12tp disconnect-cause-summary
<clear-12tp-disconnect-cause-summary>
clear services 12tp tunnel
<clear-12tp-tunnel-information>
clear services 12tp user
<clear-12tp-user-session-information>
clear services local-policy-decision-function
clear services local-policy-decision-function statistics
clear services local-policy-decision-function statistics interface
<clear-local-policy-decision-function-statistics-interface>
clear services local-policy-decision-function statistics subscriber
<clear-local-policy-decision-function-statistics-subscriber>
clear services server-load-balance
<clear-external-manager-statistics>
clear services server-load-balance hash-table
<clear-hash-table-information>
clear services server-load-balance health-monitor-statistics>
<clear-health-monitor-statistics>
clear services server-load-balance real-server-group-statistics
<clear-real-server-group-statistics>
clear services server-load-balance real-server-statistics
<clear-real-server-statistics>
clear services server-load-balance sticky
<clear-sticky-table>
clear services server-load-balance virtual-server-statistics>
<clear-virtual-server-statistics>
clear services service-sets statistics integrity-drops
<clear-service-set-syslog-statistics>
clear services service-sets statistics syslog
<clear-service-set-syslog-statistics>
clear services service-sets statistics tcp
<clear-service-tcp-tracker-statistics>
clear services stateful-firewall flow-analysis
<clear-service-flow-analysis>
clear services stateful-firewall flows
<clear-service-sfw-flow-table-information>
clear services stateful-firewall sip-call
<clear-service-sfw-sip-call-information>
clear services stateful-firewall sip-register
<clear-service-sfw-sip-register-information>
clear services stateful-firewall statistics
<clear-stateful-firewall-statistics>
clear services stateful-firewall subscriber-analysis
<clear-service-subs-analysis>
clear services subscriber
clear services subscriber sessions
<get-services-subscriber-sessions>
clear services video-monitoring
<clear-service-video-monitoring-information>
clear services video-monitoring mdi
<clear-service-video-monitoring-mdi-information>
clear services video-monitoring mdi alarm
<clear-service-video-monitoring-mdi-alarm-information>
clear services video-monitoring mdi alarm errors
<clear-services-video-monitoring-mdi-alarm-errors>
clear services video-monitoring mdi alarm stats
<clear-services-video-monitoring-mdi-alarm-stats>
clear services video-monitoring mdi errors
<clear-service-video-monitoring-mdi-errors>
clear services video-monitoring mdi statistics
<clear-service-video-monitoring-mdi-statistics>
clear services sessions analysis
<clear-service-msp-session-analysis-information>
clear services softwire
<clear-services-softwire-statistics>
clear services stateful-firewall
<clear-service-flow-analysis>
clear services stateful-firewall flows
<clear-service-sfw-flow-table-information>
clear services pgcp
<clear-service-pgcp-gates>
clear services pgcp gates
<clear-service-pgcp-gates>
clear services pgcp gates gateway
<clear-service-pgcp-gates-gateway>
clear services pgcp statistics
<clear-service-pgcp-statistics>
clear services pgcp statistics gateway
<clear-service-pgcp-statistics-gateway>
<clear-rfc2544-information>
<clear-aborted-tests-information>
<clear-active-tests-information>
clear sflow
clear sflow collector
clear sflow collector statistics
<clear-sflow-collector-statistics>
clear shmlog
clear shmlog all-info
<clear-shmlog-all-information>
clear shmlog entries
<clear-shmlog-entries>
clear shmlog statistics
<clear-shmlog-statistics>
clear snmp
clear snmp history
<clear-snmp-history>
<clear-health-monitor-routing-engine-history>.
clear snmp statistics
<clear-snmp-statistics>
clear spanning-tree
clear spanning-tree protocol-migration
clear spanning-tree protocol-migration interface
<clear-interface-stp-protocol-migration>
clear spanning-tree statistics
<clear-stp-interface-statistics>
clear spanning-tree statistics bridge
clear spanning-tree statistics interface
clear spanning-tree statistics routing-instance
<clear-stp-routing-instance-statistics>
clear spanning-tree stp-buffer
clear spanning-tree topology-change-counter
<clear-stp-topology-change-counter>
clear synchronous-ethernet
clear synchronous-ethernet esmc
clear synchronous-ethernet esmc statistics
clear system
clear system boot-media
<clear-boot-media>
clear system login
clear system login lockout
< clear-system-login-lockout>
clear-twamp-information
clear-twamp-server-information
clear-twamp-server-connection-information
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
<clear-mobile-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
<clear-mobile-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear validation
clear validation database
<clear-validation-database>
clear validation session
<clear-validation-session>
clear validation statistics
<clear-validation-statistics>
clear virtual-chassis
clear virtual-chassis heartbeat
<clear-virtual-chassis-heartbeat-statistics>
<clear virtual-chassis protocol>
clear virtual-chassis protocol statistics
<clear-virtual-chassis-statistics>
<clear-virtual-chassis-port-statistics>
clear vpls
clear vpls mac-address
<clear-vpls-mac-address>
clear vpls mac-table
<clear-vpls-mac-table>
clear vpls mac-table interface
<clear-vpls-interface-mac-table>
request interface rebalance
request pppoe
request pppoe connect
request pppoe disconnect
request security ike debug-disable
<get-disable-ike-debug>
request security ike debug-enable
<get-enable-ike-debug>
request services rpm twamp start
request services rpm twamp start client
<twamp-test-start>
request services rpm twamp stop
request services rpm twamp stop client
<twamp-test-stop>
request snmp
<request-snmp-utility-mib-clear>
<request-snmp-utility-mib-set>
clear vpls statistics
<clear-vpls-statistics>
clear vrrp
<clear-vrrp-information>
clear vrrp interface
<clear-vrrp-interface-statistics>
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
clear services inline stateful-firewall
clear services inline stateful-firewall flows
<clear-service-inline-sfw-flow-table-information>
clear services inline stateful-firewall statistics
<clear-inline-stateful-firewall-statistics>
clear services service-sets statistics drop-flow-limit
<clear-service-set-drop-flow-statistics>
clear services service-sets statistics jflow-log
<clear-service-set-jflow-log-statistics>
request services ipsec-vpn ipsec
request services ipsec-vpn ipsec switch
request services ipsec-vpn ipsec switch tunnel
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Understanding Junos OS Access Privilege Levels | 118
- Example: Configuring User Permissions with Access Privilege Levels | 124
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

configure

Can enter configuration mode.
**Commands**

```plaintext
configure
request snmp
request-snmp-utility-mib-clear
request-snmp-utility-mib-set
```

**Configuration Hierarchy Levels**

No associated CLI configuration hierarchy levels and statements.

**RELATED DOCUMENTATION**

- [Understanding Junos OS Access Privilege Levels](#)  | 118
- [Example: Configuring User Permissions with Access Privilege Levels](#)  | 124
- [Example: Configuring User Permissions with Access Privileges for Operational Mode Commands](#)  | 145
- [Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies](#)  | 160

**control**

Can perform all control-level operations; can modify any configuration.

**Commands**

```plaintext
request jnu
request jnu role
request jnu schema
```
Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

- Understanding Junos OS Access Privilege Levels | 118
- Example: Configuring User Permissions with Access Privilege Levels | 124
- Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
- Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

field

Can view field debug commands.

Commands

No associated CLI commands.

Configuration Hierarchy Levels
No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

| Understanding Junos OS Access Privilege Levels | 118 |
| Example: Configuring User Permissions with Access Privilege Levels | 124 |
| Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145 |
| Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160 |

firewall

Can view the firewall filter configuration in configuration mode.

Commands

```plaintext
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
```
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
call-trace
<monitor-mobile-gateways-call-trace-start>
call-trace clear
<get-mobile-gateways-call-trace-clear>
call-trace show
<get-mobile-gateways-call-trace-information>
call-trace start
<get-mobile-gateways-call-trace-start-information>
call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
call-trace
<get-mobile-gateways-sgw-call-trace-clear>
call-trace show
<get-mobile-gateways-sgw-call-trace-information>
call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
call-trace
<get-mobile-gateways-tdf-call-trace-clear>
call-trace show
<get-mobile-gateways-tdf-call-trace-information>
call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show firewall
<get-firewall-information>
show firewall counter
<get-firewall-counter-information>
show firewall filter
<get-firewall-filter-information>
show firewall filter version
<get-filter-version>
show firewall log
    <get-firewall-log-information>

show firewall prefix-action-stats
    <get-firewall-prefix-action-information>

show policer
    <get-policer-information>

Configuration Hierarchy Levels

[edit chassis satellite-management]
[edit firewall]
[edit dynamic-profiles firewall]
[edit firewall]
[edit logical-systems firewall]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
firewall-control | 1159
firewall-control

Can view and configure firewall filter information at the [edit dynamic-profiles firewall], [edit firewall], and [edit logical-systems firewall] hierarchy levels.

Commands

```
show firewall
   <get-firewall-information>

show firewall counter
   <get-firewall-counter-information>

show firewall filter
   <get-firewall-filter-information>

show firewall filter version
   <get-filter-version>

show firewall log
   <get-firewall-log-information>

show firewall prefix-action-stats
   <get-firewall-prefix-action-information>

show policer
```

Configuration Hierarchy Levels

```
[edit dynamic-profiles firewall]
[edit firewall]
[edit logical-systems firewall]
```

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Can read from and write to the removable media.

**Commands**

No associated CLI commands.

**Configuration Hierarchy Levels**

No associated CLI configuration hierarchy levels and statements.
Can view the flow-tap configuration in configuration mode.

**Commands**

```plaintext
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
<clear-mobile-gateway-aaa-diam-ne-statistics>
```
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
Configuration Hierarchy Levels

[edit services flow-tap]
[edit services radius-flow-tap]
[edit system services flow-tap-dtcp]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
flow-tap-control | 1165

flow-tap-control

Can view the flow-tap configuration in configuration mode and can configure flow-tap configuration information at the [edit services flow-tap], [edit services radius-flow-tap], and [edit system services flow-tap-dtcp] hierarchy levels.
Commands

No associated CLI commands.

Configuration Hierarchy Levels

[edit services flow-tap]
[edit services radius-flow-tap]
[edit system services flow-tap-dtcp]

flow-tap-operation

Can make flow-tap requests to the router.

Commands

No associated CLI commands.

Configuration Hierarchy Levels
No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

idp-profiler-operation

Can view profiler data.

Commands

No associated CLI commands.

CLI Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.
Can view the interface configuration in configuration mode.

**Commands**

```plaintext
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
<clear-mobile-gateway-sm-ippool-sessions>
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter dcca-gy
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
```

1168
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>

Configuration Hierarchy Levels

[edit accounting-options]
[edit chassis]
[edit class-of-service]
[edit class-of-service interfaces]
[edit dynamic-profiles class-of-service]
[edit dynamic-profiles class-of-service interfaces]
[edit dynamic-profiles interfaces]
[edit dynamic-profiles routing-instances instance system services dhcp-local-server]
[edit dynamic-profiles routing-instances instance system services static-subscribers group]
[edit forwarding-options]
[edit interfaces]
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services dhcp-local-server]
[edit logical-systems routing-instances instance system services static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
interface-control

Can view chassis, class of service (CoS), groups, forwarding options, and interfaces configuration information. Can edit configuration at the [edit chassis], [edit class-of-service], [edit groups], [edit forwarding-options], and [edit interfaces] hierarchy levels.

**Commands**

No associated CLI commands.

**Configuration Hierarchy Levels**

[edit accounting-options]
[edit chassis]
[edit class-of-service]
[edit class-of-service interfaces]
[edit dynamic-profiles class-of-service]
[edit dynamic-profiles class-of-service interfaces]
[edit dynamic-profiles interfaces]
[edit dynamic-profiles routing-instances instance system services dhcp-local-server]
[edit dynamic-profiles routing-instances instance system services static-subscribers group]
[edit forwarding-options]
[edit interfaces]
[edit jnx-example]
[edit logical-systems forwarding-options]
[edit logical-systems interfaces]
[edit logical-systems routing-instances instance system services dhcp-local-server]
[edit logical-systems routing-instances instance system services static-subscribers group]
[edit logical-systems system services dhcp-local-server]
[edit logical-systems system services static-subscribers group]
[edit routing-instances instance system services dhcp-local-server]
[edit routing-instances instance system services static-subscribers group]
[edit services logging]
[edit services radius-flow-tap]
[edit services radius-flow-tap interfaces]
[edit system services dhcp-local-server]
[edit system services static-subscribers group]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

interface | 1168
Can perform system maintenance, including starting a local shell on the router and becoming the superuser in the shell, and can halt and reboot the router.

**Commands**

```plaintext
clear system commit synchronize-server pending-jobs
<clear-pending-commit-sync-jobs>
clear system reboot
<clear-reboot>
clear-system-services-reverse-information
file archive
<file-archive>
file change-owner
<file-change-owner>
<extract-file>
monitor traffic
request chassis afeb
request chassis beacon
<request-chassis-beacon>
request chassis cb
<request-chassis-cb>
request chassis ccg
<request-chassis-ccg>
request chassis cfeb
request chassis cfeb master
request chassis cip
request chassis fabric
request chassis fabric device
request chassis fabric guided-cabling
request chassis fabric plane
request chassis fabric upgrade-bandwidth
request chassis fabric upgrade-bandwidth fpc
request chassis fabric upgrade-bandwidth info
request chassis fan-tray
request chassis feb
<request-feb>
```
request chassis fpc
$request-chassis-fpc
request chassis fpc optical-module
$request-fpc-optical-module
request chassis fpc optical-module amplifier-chain
$request-fpc-optical-module-amplifier-chain
request chassis fpc optical-module amplifier-chain ila
$request-fpc-optical-module-ila
request chassis fpc optical-module amplifier-chain ila firmware-upgrade
$request-fpc-optical-module-ila-firmware-upgrade
request chassis fpc optical-module amplifier-chain ila hard-reset
$request-fpc-optical-module-ila-hard-reset
request chassis fpc optical-module amplifier-chain ila soft-reset
$request-fpc-optical-module-ila-soft-reset
request chassis fpc optical-module firmware-upgrade
$request-fpc-optical-module-firmware-upgrade
request chassis fpm
request chassis mcs
request chassis mic
request chassis optics
request chassis pcg
request chassis pic
$request-chassis-pic
request chassis port-led
request chassis port-led start
$request-chassis-port-led-switch-on
request chassis port-led stop
$request-chassis-port-led-switch-off
request chassis redundancy
request chassis redundancy feb
$request-redundancy-feb
request chassis routing-engine
$request-chassis-routing-engine
request chassis routing-engine hard-disk-test
request chassis routing-engine master
request chassis satellite device-mode
request chassis satellite disable
$request-chassis-satellite-disable
request chassis satellite enable
$request-chassis-satellite-enable
request chassis satellite file-copy
<request-chassis-satellite-file-copy>
request chassis satellite install
<request-chassis-satellite-install>
request chassis satellite interface
request chassis satellite login
<request-chassis-satellite-login>
request chassis satellite reboot
<request-chassis-satellite-reboot>
request chassis satellite restart
<request-chassis-satellite-restart>
request chassis satellite restart process
request chassis satellite shell-command
<request-chassis-satellite-shell-command>

request chassis scg
request chassis sfb
request chassis sfm
request chassis sfm master
request chassis sib
<request-chassis-sib>
request chassis sib f13

request chassis sib f2s
request chassis sib optics
request chassis spmb
<request-chassis-spmb>
request chassis ssb
request chassis ssb master
request chassis synchronization
request chassis synchronization force
request chassis synchronization force automatic-switching
request chassis synchronization force mark-failed
request chassis synchronization force unmark-failed
request chassis synchronization switch
request chassis tfeb
request chassis vcpu
request chassis vnpu
request diagnostics
request diagnostics tdr
request diagnostics tdr abort
request diagnostics tdr abort interface
<abort-tdr-interface-diagnostics>
request diagnostics tdr start
request diagnostics tdr start interface
<request-tdr-interface-diagnostics>
request extension-service
request extension-service start
<extension-service-start>
request extension-service stop
<extension-service-stop>
request 12circuit-switchover
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
<request-mpls-lsp-autobandwidth-adjust>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
<reload-eedebug-action-profile>
request security idp
<request-idp-security-policy-load>
request security idp security-package
request security idp security-package download
<request-idp-security-package-download>
request security idp security-package download version
<request-idp-security-package-download-version>
request security idp security-package install
<request-idp-security-package-install>
request security idp security-package offline-download
<request-idp-security-package-offline-download>
request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
<request-idp-ssl-key-add>
request security idp ssl-inspection key delete
<request-idp-ssl-key-delete>
request security idp storage-cleanup
 <request-idp-storage-cleanup>
request security ike
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate ca-profile-group
request security pki ca-certificate ca-profile-group load
request security pki ca-certificate enroll
request security pki local-certificate export
request security pki ca-certificate load
 <load-pki-ca-certificate>
request security pki ca-certificate verify
 <verify-pki-ca-certificate>
request security pki crl
request security pki crl load
 <load-pki-crl>
request security pki generate-certificate-request
 <generate-pki-certificate-request>
request security pki generate-key-pair
 <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
 <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
 <load-pki-local-certificate>
request security pki local-certificate verify
 <verify-pki-local-certificate>
request security pki verify-integrity-status
 <verify-integrity-status>
request services fips
request services fips authorize
request services fips authorize pic
request services fips zeroize
request services fips zeroize pic
request services flow-collector
request services flow-collector change-destination
 <request-services-flow-collector-destination>
request services ggsn
request services ggsn pdp
request services ggsn pdp terminate
request services ggsn pdp terminate apn
  <request-ggsn-terminate-contexts-apn>

request services ggsn pdp terminate context
  <request-ggsn-terminate-context>

request services ggsn pdp terminate context msisdn
  <request-ggsn-terminate-msisdn-context>

request services ggsn restart
request services ggsn restart interface
  <request-ggsn-restart-interface>

request services ggsn restart node
  <request-ggsn-restart-node>

request services ggsn start
request services ggsn start interface
request services ggsn stop
request services ggsn stop interface
  <request-ggsn-stop-interface>

request services ggsn stop node
  <request-ggsn-stop-node>

request services ggsn trace
request services ggsn trace software
request services ggsn trace software update
  <request-ggsn-software-update>

request services ggsn trace start
request services ggsn trace start imsi
  <request-ggsn-start-imsi-trace>

request services ggsn trace start msisdn
  <request-ggsn-start-msisdn-trace>

request services ggsn trace stop
request services ggsn trace stop all
  <request-ggsn-stop-trace-activity>
request services ggsn trace stop imsi
   <request-ggsn-stop-imsi-trace>

request services ggsn trace stop msisdn
   <request-ggsn-stop-msisdn-trace>

request support
request support information
request system
request system boot-media
   <request-boot-media>
request system certificate
request system certificate add
request system commit
request system commit server
request system commit server pause
   <request-commit-server-pause>
request system commit server queue
request system commit server queue cleanup
   <request-commit-server-cleanup>
request system commit server start
   <request-commit-server-start>
request system configuration
request system configuration rescue
request system configuration rescue delete
   <request-delete-rescue-configuration>

request system configuration rescue save
   <request-save-rescue-configuration>
request system decrypt
   <security-decrypt-password>
request system diagnostics
request system diagnostics log-archive
   <request-log>
request system diagnostics transfer-control
   <transfer-control>
request system firmware
request system firmware downgrade
request system firmware downgrade cb
   <request-fpc-fpga-upgrade>
request system firmware downgrade cb i2c
<request-i2c-fpga-upgrade>
  request system firmware downgrade feb
  request system firmware downgrade fpc
  request system firmware downgrade pic
  request system firmware downgrade poe
  request system firmware downgrade re
  request system firmware downgrade scb
  request system firmware downgrade sfm
  request system firmware downgrade spmb
  request system firmware downgrade ssp
  request system firmware downgrade vcpu
  request system firmware upgrade
  request system firmware upgrade cb i2c
  <request-i2c-fpga-upgrade>
  request system firmware upgrade feb
  request system firmware upgrade fpc
  request system firmware upgrade fpga
  request system firmware upgrade fpga cb
  <request-cb-fpga-upgrade>
  request system firmware upgrade fpga fpc
  request system firmware upgrade fpga fpd
  <request-fpd-fpga-upgrade>
  request system firmware upgrade fpga ftc
  <request-ftc-fpga-upgrade>
  request system firmware upgrade fpga re
  <request-re-fpga-upgrade>
  request system firmware upgrade fpga scb
  <request-scb-fpga-upgrade>
  request system firmware upgrade fpga sib
  <request-sib-fpga-upgrade>
  request system firmware upgrade pic
  request system firmware upgrade poe
  request system firmware upgrade re
  request system firmware upgrade re bios
  request system firmware upgrade scb
  request system firmware upgrade sfm
  request system firmware upgrade spmb
  request system firmware upgrade ssp
  request system firmware upgrade vcpu
  request system halt
  <request-halt>
request system keep-alive
request system license
request system license add
request system license delete
  <request-license-delete>
request system license revoke-licenses
  <license-revoke-licenses>
request system license save
request system license update
  <request-license-update>
request system logout
request system logs
  <request-system-logs-copy>
request system partition
request system partition abort
request system partition compact-flash
request system partition hard-disk
request system power-off
  <request-power-off>
request system power-on
  <request-power-on-other-re>
request system process
request system process terminate
  <request-process-terminate>
request system reboot
  <request-reboot>
request system recover
request system scripts
request system scripts add
  <request-scripts-package-add>
request system scripts convert
request system scripts convert slax-to-xslt
request system scripts convert xslt-to-slax
request system scripts delete
  <request-scripts-package-delete>
request system scripts event-scripts
request system scripts event-scripts reload
  <reload-event-scripts>

request system scripts refresh-from
  <request-script-refresh-from>

request system scripts rollback
  <request-scripts-package-rollback>

request system scripts synchronize
  <request-scripts-synchronize>

request system snapshot
  <request-snapshot>

request system software
request system software abort
request system software abort in-service-upgrade
  <abort-in-service-upgrade>

request system software add
  <request-package-add>

request system software delete
  <request-package-delete>

request system software delete-backup
  <request-package-delete-backup>

request system software in-service-upgrade
  <request-package-in-service-upgrade>

request system software nonstop-upgrade
  <request-package-nonstop-upgrade>

request system software recovery-package
request system software recovery-package add
request system software recovery-package delete
request system software recovery-package extract
request system software recovery-package extract ex-8200-package
request system software recovery-package extract ex-xre200-package
request system software rollback
<request-package-rollback>

request system software validate
 <request-package-validate>
request system software validate in-service-upgrade
 <check-in-service-upgrade>

request system storage
request system storage cleanup
 <request-system-storage-clean-up>
request system storage cleanup qfabric
 <remove-qfabric-repository-contents>
request system storage mount
 <request-mount>
request system storage unified-edge
request system storage unified-edge charging
request system storage unified-edge charging media
request system storage unified-edge media
request system storage unified-edge media eject
request system storage unified-edge media prepare
request system storage unmount
 <request-unmount>
request system subscriber-management
request system subscriber-management new-sessions-disable
 <request-sm-new-sessions-disable>
request system subscriber-management new-sessions-enable
 <request-sm-new-sessions-enable>
request system yang enable
 <request-yang-enable>
request system yang update
 <request-yang-update>
request system yang validate
 <request-yang-validate>
request system zeroize
request vmhost
request vmhost cleanup
 <request-vmhost-file-cleanup>
request vmhost file-copy
 <request-vmhost-file-copy>
request vmhost halt
 <request-vmhost-halt>
request vmhost hard-disk-test
<request-vmhost-hard-disk-test>
request vmhost power-off
<request-vmhost-poweroff>
request vmhost power-on
<request-power-on-other-re>
request vmhost reboot
<request-vmhost-reboot>
request vmhost snapshot
<request-vmhost-snapshot>
request vmhost snapshot partition
<request-vmhost-snapshot-partition>
request vmhost snapshot recovery
<request-vmhost-snapshot-recovery>
request vmhost snapshot recovery partition
<request-vmhost-snapshot-recovery-partition>
request vmhost software
request vmhost software abort
request vmhost software abort in-service-upgrade
<abort-in-service-upgrade>
request vmhost software add
<request-vmhost-package-add>
request vmhost software in-service-upgrade
<request-vmhost-package-in-service-upgrade>
request vmhost software rollback
<request-package-rollback>
request vmhost zeroize
<request-vmhost-zeroize>
request vpls-switchover
set date
set date ntp
show chassis usb
show chassis usb storage
<get-usb-storage-status>
show services fips
show system configuration database
show system configuration database usage
<get-database-usage>
start shell
start shell user
test access
test access profile
    <get-radius-profile-access-test-result>
test access radius-server
   <get-radius-server-access-test-result>
get-test-services-l2tp-tunnel-result

configuration hierarchy levels

[edit event-options]
[edit security ipsec internal]
[edit security ipsec trusted-channel]
[edit services dynamic-flow-capture traceoptions]
[edit services ggsn]
[edit system fips]
[edit services ggsn rule-space]
[edit system processes daemon-process command]
[edit system scripts]
[edit system scripts commit]
[edit system scripts op]
[edit system scripts snmp]

related documentation

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

network

Can access the network by using the ping, ssh, telnet, and traceroute commands.
mtrace
mtrace from-source
mtrace monitor
mtrace to-gateway
ping
  <ping>

ping atm
ping clns
ping ethernet
  <request-ping-ethernet>
ping fibre-channel
ping mpls
ping mpls bgp
  <request-ping-bgp-lsp>
ping mpls 12circuit
ping mpls 12circuit interface
  <request-ping-12circuit-interface>
ping mpls 12circuit virtual-circuit
  <request-ping-12circuit-virtual-circuit>
ping mpls 12vpn
ping mpls 12vpn fec129
ping mpls 12vpn fec129 interface
  <request-ping-12vpn-fec129-interface>
ping mpls 12vpn instance
  <request-ping-12vpn-instance>
ping mpls 12vpn interface
  <request-ping-12vpn-interface>
ping mpls 13vpn
  <request-ping-13vpn>
ping mpls ldp
  <request-ping-ldp-lsp>
ping mpls ldp p2mp
  <request-ping-ldp-p2mp-lsp>
ping mpls lsp-end-point
    <request-ping-lsp-end-point>

ping mpls rsvp
    <request-ping-rsvp-lsp>

ping overlay
    <request-ping-overlay>
ping vpls
ping vpls instance
    <request-ping-vpls-instance>

request routing-engine
request routing-engine login
    <request-routing-engine-login>
request routing-engine login other-routing-engine
    <request-login-to-other-routing-engine>
request services flow-collector
request services flow-collector test-file-transfer
    <request-services-flow-collector-test-file-transfer>

show host
show interfaces level-extra descriptions
show multicast mrtinfo
ssh
telnet
traceroute
    <traceroute>

traceroute clns
traceroute ethernet
    <request-traceroute-ethernet>

traceroute monitor
traceroute mpls
traceroute mpls 12vpn
    <traceroute-mpls-12vpn>
traceroute mpls 12vpn fec129
    <traceroute-mpls-mspw>
traceroute mpls ldp
    <traceroute-mpls-ldp>
traceroute mpls rsvp
<traceroute-mpls-rsvp>
traceroute overlay
$request-traceroute-overlay>

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

pgcp-session-mirroring

Can view session mirroring configuration by using the pgcp command.

Commands

clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
  <clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
  clear unified-edge ggsn-pgw address-assignment pool
  <clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
  <clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
  clear unified-edge ggsn-pgw call-admission-control statistics
  <clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
  clear unified-edge ggsn-pgw charging cdr
  <clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
  <clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
  clear unified-edge ggsn-pgw charging local-persistent-storage statistics
  <clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
  clear unified-edge ggsn-pgw charging path statistics
  <clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
  clear unified-edge ggsn-pgw charging transfer statistics
  <clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
  clear unified-edge ggsn-pgw diameter dcca-gy
  clear unified-edge ggsn-pgw diameter dcca-gy statistics
  <clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
  clear unified-edge ggsn-pgw diameter network-element statistics
  <clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
  clear unified-edge ggsn-pgw diameter pcc-gx statistics
  <clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
  clear unified-edge ggsn-pgw diameter peer statistics
  <clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
  clear unified-edge ggsn-pgw gtp peer
  clear unified-edge ggsn-pgw gtp peer statistics
  <clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers charging peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw call-admission-control
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
<clear-mobile-sgw-ip-reassembly-statistics>
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf

clear unified-edge tdf aaa

clear unified-edge tdf aaa radius

clear unified-edge tdf aaa radius client

clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element

clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server

clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment

clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment

clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control

clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter

clear unified-edge tdf diameter network-element

clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx

clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
task unified-edge ggsn-pgw
task unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
task unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
task unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
task unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
task unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
task unified-edge sgw
task unified-edge sgw call-trace
task unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
task unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
task unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
task unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
task unified-edge tdf
task unified-edge tdf call-trace
task unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
task unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
task unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
task unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show services pgcp gates gate-way display session-mirroring

Configuration Hierarchy Levels
[edit services pgcp gateway session-mirroring]
[edit services pgcp session-mirroring]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
pgcp-session-mirroring-control | 1195

**pgcp-session-mirroring-control**

Can modify PGCP session mirroring configuration

**Commands**

```
show services pgcp gates gate-way display session-mirroring
```

**Configuration Hierarchy Levels**

```
[edit services pgcp gateway session-mirroring]
[edit services pgcp session-mirroring]
```
reset

Can restart software processes by using the `restart` command and can configure whether software processes configured at the [edit system processes] hierarchy level are enabled or disabled.

Commands

```plaintext
request chassis cf eb master switch
request chassis cf eb master switch no-confirm
request chassis routing-engine master acquire
request chassis routing-engine master acquire force
request chassis routing-engine master acquire force no-confirm
request chassis routing-engine master acquire no-confirm
request chassis routing-engine master release
request chassis routing-engine master release no-confirm
request chassis routing-engine master switch
request chassis routing-engine master switch no-confirm
request chassis satellite install no-confirm
request chassis sfm master switch
request chassis sfm master switch no-confirm
request chassis ssb master switch
request chassis ssb master switch no-confirm
restart
restart kernel-replication
  <restart-kernel-replication>
restart-named-service
restart routing
<routing-restart>
```
restart services
restart services border-signaling-gateway
<restart-border-signaling-gateway-service>
restart services pgcp
<restart-pgcp-service>
restart web-management
<restart-web-management>

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118

Example: Configuring User Permissions with Access Privilege Levels | 124

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145

Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

rollback

Can roll back to previous configurations.

Commands

rollback
Configuration Hierarchy Levels

[edit]

RELATED DOCUMENTATION

| Understanding Junos OS Access Privilege Levels | 118 |
| Example: Configuring User Permissions with Access Privilege Levels | 124 |
| Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145 |
| Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160 |

routing

Can view general routing, routing protocol, and routing policy configuration information.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
```
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dccca-gy
clear unified-edge ggsn-pgw diameter dccca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request mpls
request mpls lsp
request mpls lsp adjust-autobandwidth
:request-mpls-lsp-autobandwidth-adjust>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>

Configuration Hierarchy Levels
[edit bridge-domains]
[edit bridge-domains domain multicast-snooping-options]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles routing-instances]
[edit dynamic-profiles routing-instances instance bridge-domains]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options]
[edit dynamic-profiles routing-instances instance multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance pbb-options]
[edit dynamic-profiles routing-instances instance protocols]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[[edit dynamic-profiles routing-instances instance routing-options]
[edit dynamic-profiles routing-instances instance routing-options multicast traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance service-groups]
[edit dynamic-profiles routing-instances instance switch-options]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit jnx-example]
[edit fabric protocols]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols 12circuit traceoptions]
[edit logical-systems protocols 12iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols mvpn traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp lsp-set]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance igmp-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols evpn traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols rsvp]
[edit logical-systems routing-instances instance protocols rsvp lsp-set traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options validation group session traceoptions]
[edit logical-systems routing-instances instance routing-options validation traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-options validation group session traceoptions]
[edit logical-systems routing-options validation traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
[edit logical-systems vlans]
[edit logical-systems vlans vlan multicast-snooping-options]
[edit logical-systems vlans vlan multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans vlan multicast-snooping-options]
[edit logical-systems routing-instances instance vlans vlan multicast-snooping-options traceoptions]
[edit logical-systems routing-options vlans vlans vlan multicast-snooping-options]
[edit logical-systems vlans vlan multicast-snooping-options traceoptions]
[edit logical-systems vlans vlan multicast-snooping-options traceoptions]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections]
[edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvdp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit routing-instances instance multicast-snooping-options]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols evpn traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols mld-snooping traceoptions]
[edit routing-instances instance protocols mld-snooping vlan traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options]
[edit routing-instances instance routing-options validation group session traceoptions]
[edit routing-instances instance routing-options validation traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-instances instance vlans]
[edit routing-instances instance vlans vlan multicast-snooping-options]
[edit routing-instances instance vlans vlan multicast-snooping-options traceoptions]
[edit routing-options]
[edit routing-options validation group session]
[edit routing-options multicast traceoptions]
[edit routing-options validation]
[edit routing-options traceoptions]
[edit switch-options]
[edit unified-edge]
[edit vlans]
[edit vlans vlan multicast-snooping-options]
[edit vlans vlan multicast-snooping-options traceoptions]
RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

routing-control | 1209

routing-control

Can view general routing, routing protocol, and routing policy configuration information and can configure general routing at the [edit routing-options] hierarchy level, routing protocols at the [edit protocols] hierarchy level, and routing policy at the [edit policy-options] hierarchy level.

Commands

No associated CLI commands.

Configuration Hierarchy Levels

[edit bridge-domains]
[edit bridge-domains domain multicast-snooping-options]
[edit bridge-domains domain multicast-snooping-options traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles routing-instances]
[edit dynamic-profiles routing-instances instance bridge-domains]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options]
[edit dynamic-profiles routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit fabric routing-instances instance routing-options]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options]
[edit fabric routing-options traceoptions]
[edit logical-systems bridge-domains]
[edit logical-systems bridge-domains domain multicast-snooping-options]
[edit logical-systems bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems policy-options]
[edit logical-systems protocols]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iw traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances]
[edit logical-systems routing-instances instance bridge-domains]
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options]
[edit logical-systems routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance forwarding-options satellite]
[edit logical-systems routing-instances instance multicast-snooping-options]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance pbb-options]
[edit logical-systems routing-instances instance protocols]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance service-groups]
[edit logical-systems routing-instances instance switch-options]
[edit logical-systems routing-options]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems switch-options]
[edit multicast-snooping-options]
[edit multicast-snooping-options traceoptions]
[edit policy-options]
[edit protocols]
[edit protocols amt traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols connections]
[edit protocols dot1x]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols igmp-snooping]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iwl traceoptions]
[edit protocols ldp traceoptions]
[edit protocols lldp]
[edit protocols lldp-med]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols mstp]
[edit protocols mvrp]
[edit protocols oam]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp traceoptions]
[edit protocols sflow]
[edit protocols stp]
[edit protocols uplink-failure-detection]
[edit protocols vstp]
[edit routing-instances]
[edit routing-instances instance bridge-domains]
[edit routing-instances instance bridge-domains domain multicast-snooping-options]
[edit routing-instances instance bridge-domains domain multicast-snooping-options traceoptions]
[edit routing-instances instance multicast-snooping-options]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance pbb-options]
[edit routing-instances instance protocols]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance service-groups]
[edit routing-instances instance switch-options]
[edit routing-options]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit switch-options]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118

Example: Configuring User Permissions with Access Privilege Levels | 124

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
secret

Can view passwords and other authentication keys in the configuration.

Commands

No associated CLI commands.

clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter network-element
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter pcc-gx
<clear-diameter-peer-statistics>
clear unified-edge tdf diameter peer
<clear-tdf-statistics>
clear unified-edge tdf statistics
<clear-tdf-subscribers>
clear unified-edge tdf subscribers
<clear-mobile-gateway-tdf-subscribers-peer>
clear unified-edge tdf subscribers peer
request unified-edge
request unified-edge ggsn-pgw
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>

Configuration Hierarchy Levels

[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius clients accounting secret]
[edit access radius snoop-segments shared-secret]
[edit access radius-disconnect preauthentication-secret]
[edit access radius-disconnect secret]
[edit access radius-server preauthentication-secret]
[edit access radius-server secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
[edit dynamic-profiles interfaces interface unit ppp-options chap default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap]
[edit logical-systems interfaces interface unit ppp-options pap default-password]
[edit logical-systems interfaces interface unit ppp-options pap local-password]
[edit logical-systems routing-instances instance system services static-subscribers authentication password]
[edit logical-systems routing-instances instance system services static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication password]
[edit logical-systems system services static-subscribers group authentication password]
[edit routing-instances instance system services static-subscribers authentication password]
[edit routing-instances instance system services static-subscribers group authentication password]
[edit services ggsn apn radius accounting server secret]
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server preauthentication-secret]
[edit system accounting destination radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server preauthentication-secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius accounting-shared-secret]
[edit system services static-subscribers authentication password]
[edit system services static-subscribers group authentication password]
secret-control

Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.

Commands

No associated CLI commands.

Configuration Hierarchy Levels

[edit access profile client chap-secret]
[edit access profile client firewall-user password]
[edit access profile client l2tp shared-secret]
[edit access profile client pap-password]
[edit access profile radius-server secret]
[edit access radius-disconnect secret]
[edit dynamic-profiles interfaces interface ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface ppp-options pap default-password]
[edit dynamic-profiles interfaces interface ppp-options pap local-password]
[edit dynamic-profiles interfaces interface unit ppp-options chap
default-chap-secret]
[edit dynamic-profiles interfaces interface unit ppp-options pap
default-password]
[edit dynamic-profiles interfaces interface unit ppp-options pap
local-password]
[edit interfaces interface ppp-options chap default-chap-secret]
[edit interfaces interface ppp-options pap default-password]
[edit interfaces interface ppp-options pap local-password]
[edit interfaces interface unit ppp-options chap default-chap-secret]
[edit interfaces interface unit ppp-options pap default-password]
[edit interfaces interface unit ppp-options pap local-password]
[edit logical-systems interfaces interface unit ppp-options chap]
[edit logical-systems interfaces interface unit ppp-options pap
default-password]
[edit logical-systems interfaces interface unit ppp-options pap
local-password]
[edit logical-systems routing-instances instance system services
static-subscribers authentication password]
[edit logical-systems routing-instances instance system services
static-subscribers group authentication password]
[edit logical-systems system services static-subscribers authentication
password]
[edit logical-systems system services static-subscribers group authentication
password]
[edit routing-instances instance system services static-subscribers
authentication password]
[edit routing-instances instance system services static-subscribers
group authentication password]
[edit services ggsn apn radius accounting server secret]
[edit services ggsn apn radius authentication server secret]
[edit services ggsn radius server secret]
[edit system accounting destination radius server secret]
[edit system accounting destination tacplus server secret]
[edit system radius-server secret]
[edit system services outbound-ssh client secret]
[edit system services packet-triggered-subscribers partition-radius
accounting-shared-secret]
security

Can view security configuration.

Commands

- clear security
- clear security alarms
  - <clear-security-alarm-information>
- clear security idp
- clear security idp application-ddos
- clear security idp application-ddos cache
  - <clear-idp-appddos-cache>

- clear security idp application-identification
- clear security idp application-identification application-system-cache
  - <clear-idp-application-system-cache>
clear security idp application-statistics
   <clear-idp-applications-information>

clear security idp attack
clear security idp attack table
   <clear-idp-attack-table>

clear security idp counters
   <clear-idp-counters-by-counter-class>
   clear security idp counters action
clear security idp counters application-ddos
clear security idp counters application-identification
clear security idp counters dfa
clear security idp counters flow
clear security idp counters http-decoder
clear security idp counters ips
clear security idp counters log
clear security idp counters memory
clear security idp counters packet
clear security idp counters packet-log
clear security idp counters pdf-decoder
clear security idp counters policy-manager
clear security idp counters ssl-inspection
clear security idp counters tcp-reassembler

clear security idp ssl-inspection
clear security idp ssl-inspection session-id-cache
   <clear-idp-ssl-session-cache-information>
clear security idp status
   <clear-idp-status-information>
clear security log
   <clear-security-log-information>
clear security pki
clear security pki ca-certificate
   <clear-pki-ca-certificate>
clear security pki certificate-request
   <clear-pki-certificate-request>
clear security pki crl
   <clear-pki-crl>
clear security pki key-pair
<clear-pki-key-pair>
clear security pki local-certificate
  <clear-pki-local-certificate>
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
clear unified-edge ggsn-pgw diameter peer
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw gtp peer
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw ip-reassembly
<clear-mobile-gateway-sgw-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers charging peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw call-admission-control
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging local-persistent-storage
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging path
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>

clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius client
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter network-element
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter network-element statistics
<clear-unified-edge tdf diameter pcc-gx>
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf peer
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request security
request security certificate
<request-idp-policy-load>
request security idp security-package
<request-idp-security-package-download>
request security idp security-package download
request security idp security-package install
<request-idp-security-package-download-version>
request security idp ssl-inspection
<request-idp-ssl-key-add>
request security idp ssl-inspection key add
<request-idp-ssl-key-delete>
request security idp ssl-inspection key delete
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
  <load-pki-ca-certificate>
request security pki crl
request security pki crl load
  <request security pki crl load>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki verify-integrity-status
  <verify-integrity-status>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request system set-encryption-key
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
  <monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
  <get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
  <get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
  <get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
  <get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show security
show security alarms
<get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
<get-idp-addingos-application-information>
show security idp application-identification
show security idp application-identification application-system-cache
<get-idp-application-system-cache>
show security idp application-statistics
<get-idp-applications-information>
show security idp attack
show security idp attack description
<get-idp-attack-description-information>
show security idp attack detail
<get-idp-attack-detail-information>
show security idp attack table
<get-idp-attack-table-information>
show security idp counters
<get-idp-counter-information>
show security idp counters action
show security idp counters application-ddos
show security idp counters application-identification
show security idp counters dfa
show security idp counters flow
show security idp counters http-decoder
show security idp counters ips
show security idp counters log
show security idp counters memory
show security idp counters packet
show security idp counters packet-log
show security idp counters pdf-decoder
show security idp counters policy-manager
show security idp counters ssl-inspection
show security idp counters tcp-reassembler

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
    <get-idp-memory-information>

show security idp policies
    <get-idp-subscriber-policy-list>

show security idp policy-templates-list
    <get-idp-policy-template-information>
    <get-idp-predefined-attack-groups>
    <get-idp-predefined-attack-group-filters>
    <get-idp-predefined-attacks>
    <get-idp-predefined-attack-filters>
    <get-idp-recent-security-package-information>
show security idp policy-commit-status
    <get-idp-policy-commit-status>

<get-idp-recent-security-package-information>

show security idp ssl-inspection
    <get-idp-security-package-information>

show security idp ssl-inspection key
<get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
  <get-idp-ssl-session-cache-information>

show security idp status
  <get-idp-status-information>

show security idp status detail
  <get-idp-detail-status-information>
show security keychain
  <get-hakr-keychain-information>
show security log
  <get-security-log-information>

show security pki
show security pki ca-certificate
  <get-pki-ca-certificate>
show security pki certificate-request
  <get-pki-certificate-request>
show security pki crl
  <get-pki-crl>
show security pki local-certificate
  <get-pki-local-certificate>

Configuration Hierarchy Levels

[edit security]
[edit security alarms]
[edit security log]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels  |  118
Example: Configuring User Permissions with Access Privilege Levels  |  124
security-control

Can view and configure security information at the [edit security] hierarchy level.

Commands

- clear security
- clear security alarms
  - <clear-security-alarm-information>
- clear security idp
- clear security idp application-ddos
- clear security idp application-ddos cache
  - <clear-idp-appddos-cache>
- clear security idp application-identification
- clear security idp application-identification application-system-cache
  - <clear-idp-application-system-cache>
- clear security idp application-statistics
  - <clear-idp-applications-information>
- clear security idp attack
- clear security idp attack table
  - <clear-idp-attack-table>
- clear security idp counters
  - <clear-idp-counters-by-counter-class>
- clear security idp ssl-inspection
- clear security idp ssl-inspection session-id-cache
  - <clear-idp-ssl-session-cache-information>
- clear security idp status
<clear-idp-status-information>
clear security log
  <clear-security-log-information>
clear security pki
clear security pki ca-certificate
  <clear-pki-ca-certificate>
clear security pki certificate-request
  <clear-pki-certificate-request>
clear security pki crl
  <clear-pki-crl>
clear security pki key-pair
  <clear-pki-key-pair>
clear security pki local-certificate
  <clear-pki-local-certificate>
request security
request security certificate
request security certificate enroll
request security datapath-debug
request security datapath-debug action-profile
request security datapath-debug action-profile reload-all
request security idp
  <request-idp-policy-load>
request security idp security-package
request security idp security-package download
  <request-idp-security-package-download>
request security idp security-package download version
  <request-idp-security-package-download-version>
request security idp security-package install
  <request-idp-security-package-install>
request security idp security-package offline-download
  <request-idp-security-package-offline-download>
request security idp ssl-inspection
request security idp ssl-inspection key
request security idp ssl-inspection key add
  <request-idp-ssl-key-add>
request security idp ssl-inspection key delete
  <request-idp-ssl-key-delete>
request security idp storage-cleanup
  <request-idp-storage-cleanup>
request security key-pair
request security pki
request security pki ca-certificate
request security pki ca-certificate verify
  <verify-pki-ca-certificate>
request security pki ca-certificate enroll
request security pki ca-certificate load
  <load-pki-ca-certificate>
request security pki crl
request security pki crl load
  <request security pki crl load>
request security pki generate-certificate-request
  <generate-pki-certificate-request>
request security pki generate-key-pair
  <generate-pki-key-pair>
request security pki local-certificate
request security pki local-certificate verify
  <verify-pki-local-certificate>
request security pki local-certificate enroll
request security pki local-certificate generate-self-signed
  <generate-pki-self-signed-local-certificate>
request security pki local-certificate load
  <load-pki-local-certificate>
request system set-encryption-key
show security
show security alarms
  <get-security-alarm-information>
show security idp
show security idp application-ddos
show security idp application-ddos application
  <get-idp-addos-application-information>

show security idp application-identification
show security idp application-identification application-system-cache
  <get-idp-application-system-cache>

show security idp application-statistics
  <get-idp-applications-information>

show security idp attack
show security idp attack description
  <get-idp-attack-description-information>
show security idp attack detail
   <get-idp-attack-detail-information>
show security idp attack table
   <get-idp-attack-table-information>

show security idp counters
   <get-idp-counter-information>
show security idp counters action
show security idp counters application-ddos
show security idp counters application-identification
show security idp counters dfa
show security idp counters flow
show security idp counters http-decoder
show security idp counters ips
show security idp counters log
show security idp counters memory
show security idp counters packet
show security idp counters packet-log
show security idp counters pdf-decoder
show security idp counters policy-manager
show security idp counters ssl-inspection
show security idp counters tcp-reassembler

show security idp logical-system
show security idp logical-system policy-association
show security idp memory
   <get-idp-memory-information>

show security idp policies
   <get-idp-subscriber-policy-list>

show security idp policy-templates-list
   <get-idp-policy-template-information>
   <get-idp-predefined-attack-groups>
   <get-idp-predefined-attack-group-filters>
   <get-idp-predefined-attacks>
   <get-idp-predefined-attack-filters>
   <get-idp-recent-security-package-information>
show security idp policy-commit-status
   <get-idp-policy-commit-status>

   <get-idp-recent-security-package-information>
show security idp security-package-version
   <get-idp-security-package-information>

show security idp ssl-inspection
show security idp ssl-inspection key
   <get-idp-ssl-key-information>

show security idp ssl-inspection session-id-cache
   <get-idp-ssl-session-cache-information>

show security idp status
   <get-idp-status-information>

show security idp status detail
   <get-idp-detail-status-information>
show security keychain
   <get-hakr-keychain-information>
show security log
   <get-security-log-information>

show security pki
show security pki ca-certificate
   <get-pki-ca-certificate>
show security pki certificate-request
   <get-pki-certificate-request>
show security pki crl
   <get-pki-crl>
show security pki local-certificate
   <get-pki-local-certificate>

Configuration Hierarchy Levels

[edit security]
[edit security alarms]
[edit security log]
shell

Can start a local shell on the router.

Commands

```
start shell
start shell user
```

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.
Can view Simple Network Management Protocol (SNMP) configuration.

**Commands**

```plaintext
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter dcca-gy
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
```
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
call-trace
request unified-edge tdf call-trace
call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
call-trace information
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>

Configuration Hierarchy Levels

[edit snmp]
[edit unified-edge]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

snmp-control

Can view SNMP configuration information and can modify SNMP configuration at the [edit snmp] hierarchy level.

Commands
No associated CLI commands.

Configuration Hierarchy Levels

```
[edit snmp]
```

RELATED DOCUMENTATION

| Understanding Junos OS Access Privilege Levels | 118 |
| Example: Configuring User Permissions with Access Privilege Levels | 124 |
| Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145 |
| Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160 |

system

Can view system-level configuration information.

Commands

```
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
<clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
```
<clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
<clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
<clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
<clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
<clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
<clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
<clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
<clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
<clear-mobile-gateway-charging-clear-xfer-stats>
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
<clear-mobile-sgw>
clear unified-edge sgw call-admission-control
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
<clear-mobile-sgw-charging>
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
<clear-mobile-gateway-sgw-charging-clear-lps-stats>
clear unified-edge sgw charging path
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
<clear-mobile-sgw-gtp>
clear unified-edge sgw gtp peer
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
<clear-mobile-gw-sgw-idle-mode-buffering-stats>
clear unified-edge sgw ip-reassembly
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
<clear-mobile-sgw-subscribers>
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
request chassis synchronization
request chassis synchronization force
request chassis synchronization force automatic-switching
request chassis synchronization force mark-failed
request chassis synchronization force unmark-failed
request chassis synchronization switch
request path-computation-client retry-delegation
$request-path-computation-retry-delegation>
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
Request Unified-Edge TDF Call-Trace Information

Request Virtual-Chassis Device Reachability

Request Virtual-Chassis Member ID

Delete Virtual-Chassis Member ID

Request Virtual-Chassis Mode

Request Virtual-Chassis Mode Mixed

Request Virtual-Chassis Reactivate

Request Virtual-Chassis Recycle

Request Virtual-Chassis Renumber

Request Virtual-Chassis Routing-Engine

Request Virtual-Chassis Routing-Engine Master

Request Virtual-Chassis Routing-Engine Master Switch

Set Virtual-Chassis Mode

Request Virtual-Chassis VC-Port Delete

Request Virtual-Chassis VC-Port Delete FPC-Slot

Request Virtual-Chassis VC-Port Delete PIC-Slot

Request Virtual-Chassis VC-Port Set

Request Virtual-Chassis VC-Port Set FPC-Slot

Request Virtual-Chassis VC-Port Set Interface

Request Virtual-Chassis VC-Port Set PIC-Slot

Configuration Hierarchy Levels
[edit applications]
[edit chassis network-slices]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit fabric virtual-chassis]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems protocols uplink-failure-detection]
[edit logical-systems routing-instances instance forwarding-options helpers bootp]
[edit logical-systems routing-instances instance forwarding-options helpers domain]
[edit logical-systems routing-instances instance forwarding-options helpers port]
[edit logical-systems routing-instances instance forwarding-options helpers tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit logical-systems system syslog]
[edit poe]
[edit protocols uplink-failure-detection]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system boot loader authentication]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollbacks]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system no-debugger-on-alt-break]
[edit system no-redirects-ipv6]
[edit system name-server]
[edit no-hidden-commands system]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirects]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports auxiliary silent-with-modem]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system ports console silent-with-modem]
[edit system processes]
[edit system proxy]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit unified-edge]
[edit virtual-chassis]
[edit virtual-chassis locality-bias]
[edit vlans]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
system-control | 1252

**system-control**

Can view system-level configuration information and configure it at the [edit system] hierarchy level.

**Configuration Hierarchy Levels**

[edit applications]
[edit chassis system-domains]
[edit dynamic-profiles routing-instances instance forwarding-options helpers tftp]
[edit dynamic-profiles routing-instances instance routing-options fate-sharing]
[edit ethernet-switching-options]
[edit forwarding-options helpers bootp]
[edit forwarding-options helpers domain]
[edit forwarding-options helpers port]
[edit forwarding-options helpers tftp]
[edit logical-systems]
[edit logical-systems routing-instances instance forwarding-options helpers bootp]
[edit logical-systems routing-instances instance forwarding-options helpers domain]
[edit logical-systems routing-instances instance forwarding-options helpers port]
[edit logical-systems routing-instances instance forwarding-options helpers tftp]
[edit logical-systems routing-instances instance routing-options fate-sharing]
[edit logical-systems routing-options fate-sharing]
[edit logical-systems system]
[edit poe]
[edit routing-instances instance forwarding-options helpers bootp]
[edit routing-instances instance forwarding-options helpers domain]
[edit routing-instances instance forwarding-options helpers port]
[edit routing-instances instance forwarding-options helpers tftp]
[edit routing-instances instance routing-options fate-sharing]
[edit routing-options fate-sharing]
[edit services]
[edit services ggsn charging charging-log traceoptions]
[edit system]
[edit system archival]
[edit system backup-router]
[edit system compress-configuration-files]
[edit system default-address-selection]
[edit system dgasp-in]
[edit system dgasp-usb]
[edit system domain-name]
[edit system domain-search]
[edit system encrypt-configuration-files]
[edit system host-name]
[edit system inet6-backup-router]
[edit system internet-options gre-path-mtu-discovery]
[edit system internet-options ipip-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery]
[edit system internet-options ipv6-path-mtu-discovery-timeout]
[edit system internet-options ipv6-reject-zero-hop-limit]
[edit system internet-options no-tcp-reset]
[edit system internet-options no-tcp-rfc1323]
[edit system internet-options no-tcp-rfc1323-paws]
[edit system internet-options path-mtu-discovery]
[edit system internet-options source-port upper-limit]
[edit system internet-options source-quench]
[edit system internet-options tcp-drop-synfin-set]
[edit system internet-options tcp-mss]
[edit system license]
[edit system max-configuration-rollback]
[edit system max-configurations-on-flash]
[edit system mirror-flash-on-disk]
[edit system name-server]
[edit system no-multicast-echo]
[edit system no-neighbor-learn]
[edit system no-redirect]
[edit system ports auxiliary log-out-on-disconnect]
[edit system ports auxiliary port-type]
[edit system ports console log-out-on-disconnect]
[edit system ports console port-type]
[edit system processes]
[edit system saved-core-context]
[edit system saved-core-files]
[edit system services]
[edit system services web-management]
[edit system static-host-mapping]
[edit system syslog]
[edit system time-zone]
[edit virtual-chassis]
[edit vlans]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
system | 1244
trace

Can view trace file settings and configure trace file properties.

Commands

```
clear log
    <clear-log>
clear log satellite
    <clear-log-satellite>
clear unified-edge
clear unified-edge ggsn-pgw
clear unified-edge ggsn-pgw aaa
clear unified-edge ggsn-pgw aaa radius
clear unified-edge ggsn-pgw aaa radius statistics
    <clear-mobile-gateway-aaa-radius-statistics>
clear unified-edge ggsn-pgw aaa statistics
    <clear-mobile-gateway-aaa-statistics>
clear unified-edge ggsn-pgw address-assignment
clear unified-edge ggsn-pgw address-assignment pool
    <clear-mobile-gateway-sm-ippool-pool-sessions>
clear unified-edge ggsn-pgw address-assignment statistics
    <clear-mobile-gateway-sm-ippool-statistics>
clear unified-edge ggsn-pgw call-admission-control
clear unified-edge ggsn-pgw call-admission-control statistics
    <clear-mobile-gateway-cac-statistics>
clear unified-edge ggsn-pgw charging
clear unified-edge ggsn-pgw charging cdr
    <clear-mobile-gateway-charging-clear-cdr>
clear unified-edge ggsn-pgw charging cdr wfa
    <clear-mobile-gateway-charging-clear-cdr-wfa>
clear unified-edge ggsn-pgw charging local-persistent-storage
clear unified-edge ggsn-pgw charging local-persistent-storage statistics
    <clear-mobile-gateway-charging-clear-lps-stats>
clear unified-edge ggsn-pgw charging path
clear unified-edge ggsn-pgw charging path statistics
    <clear-mobile-gateway-charging-clear-path-stats>
clear unified-edge ggsn-pgw charging transfer
clear unified-edge ggsn-pgw charging transfer statistics
    <clear-mobile-gateway-charging-clear-xfer-stats>
```
clear unified-edge ggsn-pgw diameter
clear unified-edge ggsn-pgw diameter dcca-gy
clear unified-edge ggsn-pgw diameter dcca-gy statistics
<clear-mobile-gateway-aaa-diam-stats-gy>
clear unified-edge ggsn-pgw diameter network-element
clear unified-edge ggsn-pgw diameter network-element statistics
<clear-mobile-gateway-aaa-diam-ne-statistics>
clear unified-edge ggsn-pgw diameter pcc-gx
clear unified-edge ggsn-pgw diameter pcc-gx statistics
<clear-mobile-gateway-aaa-diam-stats-gx>
clear unified-edge ggsn-pgw diameter peer
clear unified-edge ggsn-pgw diameter peer statistics
<clear-mobile-gateway-aaa-diam-peer-statistics>
clear unified-edge ggsn-pgw gtp
clear unified-edge ggsn-pgw gtp peer
clear unified-edge ggsn-pgw gtp peer statistics
<clear-mobile-gateway-gtp-peer-statistics>
clear unified-edge ggsn-pgw gtp statistics
<clear-mobile-gateway-gtp-statistics>
clear unified-edge ggsn-pgw ip-reassembly
clear unified-edge ggsn-pgw ip-reassembly statistics
<clear-mobile-gateways-ip-reassembly-statistics>
clear unified-edge ggsn-pgw statistics
<clear-mobile-gateway-statistics>
clear unified-edge ggsn-pgw subscribers
<clear-mobile-gateway-subscribers>
clear unified-edge ggsn-pgw subscribers bearer
clear unified-edge ggsn-pgw subscribers charging
<clear-mobile-gateway-subscribers-charging>
clear unified-edge ggsn-pgw subscribers peer
<clear-mobile-gateway-subscribers-peer>
clear unified-edge sgw
clear unified-edge sgw call-admission-control
clear unified-edge sgw call-admission-control statistics
<clear-mobile-sgw-cac-statistics>
clear unified-edge sgw charging
clear unified-edge sgw charging cdr
<clear-mobile-gateway-sgw-charging-clear-cdr>
clear unified-edge sgw charging cdr wfa
<clear-mobile-gateway-sgw-charging-clear-cdr-wfa>
clear unified-edge sgw charging local-persistent-storage
clear unified-edge sgw charging local-persistent-storage statistics
clear unified-edge sgw charging path
clear unified-edge sgw charging path statistics
<clear-mobile-gateway-sgw-charging-clear-path-stats>
clear unified-edge sgw charging transfer
clear unified-edge sgw charging transfer statistics
<clear-mobile-gateway-sgw-charging-clear-xfer-stats>
clear unified-edge sgw gtp
clear unified-edge sgw gtp peer
clear unified-edge sgw gtp peer statistics
<clear-mobile-sgw-gtp-peer-statistics>
clear unified-edge sgw gtp statistics
<clear-mobile-sgw-gtp-statistics>
clear unified-edge sgw idle-mode-buffering
clear unified-edge sgw idle-mode-buffering statistics
<clear-mobile-gw-sgw-idle-mode-buffering-statistics>
clear unified-edge sgw ip-reassembly
clear unified-edge sgw ip-reassembly statistics
<clear-mobile-gateways-sgw-ip-reassembly-statistics-sgw>
clear unified-edge sgw statistics
<clear-mobile-sgw-statistics>
clear unified-edge sgw subscribers
clear unified-edge sgw subscribers charging
<clear-mobile-sgw-subscribers-charging>
clear unified-edge sgw subscribers peer
<clear-mobile-sgw-subscribers-peer>
clear unified-edge tdf
clear unified-edge tdf aaa
clear unified-edge tdf aaa radius
clear unified-edge tdf aaa radius client
clear unified-edge tdf aaa radius client statistics
<clear-radius-client-statistics>
clear unified-edge tdf aaa radius network-element
clear unified-edge tdf aaa radius network-element statistics
<clear-radius-network-element-statistics>
clear unified-edge tdf aaa radius server
clear unified-edge tdf aaa radius server statistics
<clear-radius-server-statistics>
clear unified-edge tdf aaa radius snoop-segment
clear unified-edge tdf aaa radius snoop-segment statistics
<clear-radius-snoop-segment-statistics>
clear unified-edge tdf aaa statistics
<clear-tdf-gateway-aaa-statistics>
clear unified-edge tdf address-assignment
clear unified-edge tdf address-assignment pool
<clear-mobile-gateway-tdf-sm-ippool-pool-sessions>
clear unified-edge tdf address-assignment statistics
<clear-mobile-gateway-tdf-sm-ippool-statistics>
clear unified-edge tdf call-admission-control
clear unified-edge tdf call-admission-control statistics
<clear-tdf-cac-statistics>
clear unified-edge tdf diameter
clear unified-edge tdf diameter network-element
clear unified-edge tdf diameter network-element statistics
<clear-diameter-network-element-statistics>
clear unified-edge tdf diameter pcc-gx
clear unified-edge tdf diameter pcc-gx statistics
<clear-diameter-statistics-gx>
clear unified-edge tdf diameter peer
clear unified-edge tdf diameter peer statistics
<clear-diameter-peer-statistics>
clear unified-edge tdf statistics
<clear-tdf-statistics>
clear unified-edge tdf subscribers
<clear-mobile-tdf-subscribers>
clear unified-edge tdf subscribers peer
<clear-mobile-gateway-tdf-subscribers-peer>
monitor
request-monitor-ethernet-delay-measurement
  <request-monitor-ethernet-loss-measurement>
monitor interface
monitor interface traffic
monitor label-switched-path
monitor list
monitor start
monitor static-lsp
monitor stop
request unified-edge
request unified-edge ggsn-pgw
request unified-edge ggsn-pgw call-trace
<monitor-mobile-gateways-call-trace-start>
request unified-edge ggsn-pgw call-trace clear
<get-mobile-gateways-call-trace-clear>
request unified-edge ggsn-pgw call-trace show
<get-mobile-gateways-call-trace-information>
request unified-edge ggsn-pgw call-trace start
<get-mobile-gateways-call-trace-start-information>
request unified-edge ggsn-pgw call-trace stop
<get-mobile-gateways-call-trace-stop-information>
request unified-edge sgw
request unified-edge sgw call-trace
request unified-edge sgw call-trace clear
<get-mobile-gateways-sgw-call-trace-clear>
request unified-edge sgw call-trace show
<get-mobile-gateways-sgw-call-trace-information>
request unified-edge sgw call-trace start
<get-mobile-gateways-sgw-call-trace-start-information>
request unified-edge sgw call-trace stop
<get-mobile-gateways-sgw-call-trace-stop-information>
request unified-edge tdf
request unified-edge tdf call-trace
request unified-edge tdf call-trace clear
<get-mobile-gateways-tdf-call-trace-clear>
request unified-edge tdf call-trace show
<get-mobile-gateways-tdf-call-trace-information>
request unified-edge tdf call-trace start
<get-mobile-gateways-tdf-call-trace-start-information>
request unified-edge tdf call-trace stop
<get-mobile-gateways-tdf-call-trace-stop-information>
show log
<get-log>
show log user
  <get-syslog-events>

Configuration Hierarchy Levels

[edit unified-edge]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit class-of-service application-traffic-control traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles class-of-service application-traffic-control traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management traceoptions]
[edit dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols oam gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ospf traceoptions]
[edit dynamic-profiles routing-instances instance protocols pim traceoptions]
[edit dynamic-profiles routing-instances instance protocols rip traceoptions]
[edit dynamic-profiles routing-instances instance protocols ripng traceoptions]
[edit dynamic-profiles routing-instances instance protocols router-discovery traceoptions]
[edit dynamic-profiles routing-instances instance protocols vpls traceoptions]
[edit dynamic-profiles routing-instances instance routing-options multicast traceoptions]
[edit dynamic-profiles routing-instances instance routing-options traceoptions]
[edit dynamic-profiles routing-instances instance services mobile-ip traceoptions]
[edit dynamic-profiles routing-instances instance system services dhcp-local-server traceoptions]
[edit dynamic-profiles routing-options multicast traceoptions]
[edit fabric protocols bgp group neighbor traceoptions]
[edit fabric protocols bgp group traceoptions]
[edit fabric protocols bgp traceoptions]
[edit fabric routing-instances instance routing-options traceoptions]
[edit fabric routing-options traceoptions]
[edit jnx-example traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems vlans domain forwarding-options dhcp-relay interface traceoptions]
[edit logical-systems vlans domain multicast-snooping-options traceoptions]
[edit logical-systems vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems forwarding-options dhcp-relay traceoptions]
[edit logical-systems protocols ancp traceoptions]
[edit logical-systems protocols bgp group neighbor traceoptions]
[edit logical-systems protocols bgp group traceoptions]
[edit logical-systems protocols bgp traceoptions]
[edit logical-systems protocols dot1x traceoptions]
[edit logical-systems protocols dvmrp traceoptions]
[edit logical-systems protocols esis traceoptions]
[edit logical-systems protocols igmp traceoptions]
[edit logical-systems protocols igmp-host traceoptions]
[edit logical-systems protocols ilmi traceoptions]
[edit logical-systems protocols isis traceoptions]
[edit logical-systems protocols l2circuit traceoptions]
[edit logical-systems protocols l2iwan traceoptions]
[edit logical-systems protocols lACP traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet fnp traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet fnp traceoptions]
[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp lsp-set traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance services mobile-ip traceoptions]
[edit logical-systems routing-instances instance services mobile-ip traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server service traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server interface traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server service traceoptions]
[edit logical-systems system services dhcp-local-server interface traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iw traceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols protocols oam ethernet fnp]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsvp lsp-set traceoptions]
[edit protocols rsvp traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit services l2tp traceoptions]
[edit services server-load-balance traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system ddos-protection traceoptions]
[edit system license traceoptions]
[edit system processes app-engine-virtual-machine-management-service traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes dhcp-service interface traceoptions]
[edit system processes dhcp-service traceoptions]
trace-control

Can modify trace file settings and configure trace file properties.

Configuration Hierarchy Levels
[edit vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit vlans domain forwarding-options dhcp-relay traceoptions]
[edit vlans domain multicast-snooping-options traceoptions]
[edit vlans domain protocols igmp-snooping traceoptions]
[edit demux traceoptions]
[edit dynamic-profiles protocols igmp traceoptions]
[edit dynamic-profiles protocols mld traceoptions]
[edit dynamic-profiles protocols oam ethernet link-fault-management traceoptions]
[edit dynamic-profiles protocols oam ethernet lmi]
[edit dynamic-profiles protocols protocols router-advertisement traceoptions]
[edit dynamic-profiles protocols protocols gre-tunnel traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit dynamic-profiles routing-instances instance multicast-snooping-options traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group neighbor traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols bgp traceoptions]
[edit dynamic-profiles routing-instances instance protocols esis traceoptions]
[edit dynamic-profiles routing-instances instance protocols igmp-snooping traceoptions]
[edit dynamic-profiles routing-instances instance protocols isis traceoptions]
[edit dynamic-profiles routing-instances instance protocols l2vpn traceoptions]
[edit dynamic-profiles routing-instances instance protocols ldp traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp group traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp peer traceoptions]
[edit dynamic-profiles routing-instances instance protocols msdp traceoptions]
[edit dynamic-profiles routing-instances instance protocols mvpn traceoptions]
[edit logical-systems protocols lacp traceoptions]
[edit logical-systems protocols layer2-control traceoptions]
[edit logical-systems protocols ldp traceoptions]
[edit logical-systems protocols mld traceoptions]
[edit logical-systems protocols mld-host traceoptions]
[edit logical-systems protocols mpls label-switched-path oam traceoptions]
[edit logical-systems protocols mpls label-switched-path primary oam traceoptions]
[edit logical-systems protocols mpls label-switched-path secondary oam traceoptions]
[edit logical-systems protocols mpls oam traceoptions]
[edit logical-systems protocols msdp oam traceoptions]
[edit logical-systems protocols msdp group peer traceoptions]
[edit logical-systems protocols msdp group traceoptions]
[edit logical-systems protocols msdp peer traceoptions]
[edit logical-systems protocols msdp traceoptions]
[edit logical-systems protocols neighbor-discovery secure traceoptions]
[edit logical-systems protocols oam ethernet link-fault-management traceoptions]
[edit logical-systems protocols oam ethernet lmi traceoptions]
[edit logical-systems protocols ospf traceoptions]
[edit logical-systems protocols pim traceoptions]
[edit logical-systems protocols ppp monitor-session]
[edit logical-systems protocols ppp traceoptions]
[edit logical-systems protocols ppp-service traceoptions]
[edit logical-systems protocols pppoe traceoptions]
[edit logical-systems protocols rip traceoptions]
[edit logical-systems protocols ripng traceoptions]
[edit logical-systems protocols router-advertisement traceoptions]
[edit logical-systems protocols router-discovery traceoptions]
[edit logical-systems protocols rsvp traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit logical-systems routing-instances instance vlans domain forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit logical-systems routing-instances instance multicast-snooping-options traceoptions]
[edit logical-systems routing-instances instance protocols bgp group neighbor traceoptions]
[edit logical-systems routing-instances instance protocols bgp group traceoptions]
[edit logical-systems routing-instances instance protocols bgp traceoptions]
[edit logical-systems routing-instances instance protocols esis traceoptions]
[edit logical-systems routing-instances instance protocols igmp-snooping traceoptions]
[edit logical-systems routing-instances instance protocols isis traceoptions]
[edit logical-systems routing-instances instance protocols l2vpn traceoptions]
[edit logical-systems routing-instances instance protocols ldp traceoptions]
[edit logical-systems routing-instances instance protocols msdp group peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp group traceoptions]
[edit logical-systems routing-instances instance protocols msdp peer traceoptions]
[edit logical-systems routing-instances instance protocols msdp traceoptions]
[edit logical-systems routing-instances instance protocols mvpn traceoptions]
[edit logical-systems routing-instances instance protocols ospf traceoptions]
[edit logical-systems routing-instances instance protocols pim traceoptions]
[edit logical-systems routing-instances instance protocols rip traceoptions]
[edit logical-systems routing-instances instance protocols ripng traceoptions]
[edit logical-systems routing-instances instance protocols router-discovery traceoptions]
[edit logical-systems routing-instances instance protocols vpls traceoptions]
[edit logical-systems routing-instances instance routing-options multicast traceoptions]
[edit logical-systems routing-instances instance routing-options traceoptions]
[edit logical-systems routing-instances instance routing-options mobile-ip traceoptions]
[edit logical-systems routing-instances instance services mobile-ip traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server interface-traceoptions]
[edit logical-systems routing-instances instance system services dhcp-local-server traceoptions]
[edit logical-systems routing-options multicast traceoptions]
[edit logical-systems routing-options traceoptions]
[edit logical-systems services mobile-ip traceoptions]
[edit logical-systems system services dhcp-local-server interface-traceoptions]
[edit logical-systems system services dhcp-local-server traceoptions]
[edit multicast-snooping-options traceoptions]
[edit protocols ancp traceoptions]
[edit protocols bgp group neighbor traceoptions]
[edit protocols bgp group traceoptions]
[edit protocols bgp traceoptions]
[edit protocols dot1x traceoptions]
[edit protocols dvmrp traceoptions]
[edit protocols esis traceoptions]
[edit protocols igmp traceoptions]
[edit protocols igmp-host traceoptions]
[edit protocols ilmi traceoptions]
[edit protocols isis traceoptions]
[edit protocols l2circuit traceoptions]
[edit protocols l2iwltraceoptions]
[edit protocols lacp traceoptions]
[edit protocols layer2-control traceoptions]
[edit protocols ldp traceoptions]
[edit protocols mld traceoptions]
[edit protocols mld-host traceoptions]
[edit protocols mpls label-switched-path oam traceoptions]
[edit protocols mpls label-switched-path primary oam traceoptions]
[edit protocols mpls label-switched-path secondary oam traceoptions]
[edit protocols mpls oam traceoptions]
[edit protocols msdp group peer traceoptions]
[edit protocols msdp group traceoptions]
[edit protocols msdp peer traceoptions]
[edit protocols msdp traceoptions]
[edit protocols neighbor-discovery secure traceoptions]
[edit protocols oam ethernet connectivity-fault-management traceoptions]
[edit protocols oam ethernet link-fault-management traceoptions]
[edit protocols oam ethernet lmi traceoptions]
[edit protocols ospf traceoptions]
[edit protocols pim traceoptions]
[edit protocols ppp monitor-session]
[edit protocols ppp traceoptions]
[edit protocols ppp-service traceoptions]
[edit protocols pppoe traceoptions]
[edit protocols rip traceoptions]
[edit protocols ripng traceoptions]
[edit protocols router-advertisement traceoptions]
[edit protocols router-discovery traceoptions]
[edit protocols rsrp traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay interface-traceoptions]
[edit routing-instances instance vlans domain forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance vlans domain multicast-snooping-options traceoptions]
[edit routing-instances instance vlans domain protocols igmp-snooping traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay traceoptions]
[edit routing-instances instance forwarding-options dhcp-relay interface-traceoptions]
[edit routing-instances instance multicast-snooping-options traceoptions]
[edit routing-instances instance protocols bgp group neighbor traceoptions]
[edit routing-instances instance protocols bgp group traceoptions]
[edit routing-instances instance protocols bgp traceoptions]
[edit routing-instances instance protocols esis traceoptions]
[edit routing-instances instance protocols igmp-snooping traceoptions]
[edit routing-instances instance protocols isis traceoptions]
[edit routing-instances instance protocols l2vpn traceoptions]
[edit routing-instances instance protocols ldp traceoptions]
[edit routing-instances instance protocols msdp group peer traceoptions]
[edit routing-instances instance protocols msdp group traceoptions]
[edit routing-instances instance protocols msdp peer traceoptions]
[edit routing-instances instance protocols msdp traceoptions]
[edit routing-instances instance protocols mvpn traceoptions]
[edit routing-instances instance protocols ospf traceoptions]
[edit routing-instances instance protocols pim traceoptions]
[edit routing-instances instance protocols rip traceoptions]
[edit routing-instances instance protocols ripng traceoptions]
[edit routing-instances instance protocols router-discovery traceoptions]
[edit routing-instances instance protocols vpls traceoptions]
[edit routing-instances instance routing-options multicast traceoptions]
[edit routing-instances instance routing-options traceoptions]
[edit routing-instances instance system services dhcp-local-server interface-traceoptions]
[edit routing-instances instance system services dhcp-local-server traceoptions]
[edit routing-options multicast traceoptions]
[edit routing-options traceoptions]
[edit security idp traceoptions]
[edit security pki traceoptions]
[edit services adaptive-services-pics traceoptions]
[edit services captive-portal-content-delivery]
[edit system ddos-protection traceoptions]
[edit services l2tp traceoptions]
[edit services logging traceoptions]
[edit services mobile-ip traceoptions]
[edit services server-load-balance traceoptions]
[edit services ssl traceoptions]
[edit system accounting traceoptions]
[edit system auto-configuration traceoptions]
[edit system license traceoptions]
[edit system processes datapath-trace-service traceoptions]
[edit system processes diameter-service traceoptions]
[edit system processes general-authentication-service traceoptions]
[edit system processes mac-validation traceoptions]
[edit system processes process-monitor traceoptions]
[edit system processes resource-cleanup traceoptions]
[edit system processes sdk-service traceoptions]
[edit system processes static-subscribers traceoptions]
[edit system services database-replication traceoptions]
[edit system services dhcp traceoptions]
[edit system services dhcp-local-server traceoptions]
[edit system services dhcp-local-server interface-traceoptions]
[edit system services local-policy-decision-function traceoptions]
[edit system services outbound-ssh traceoptions]
[edit system services service-deployment traceoptions]
[edit system services subscriber-management traceoptions]
[edit system services subscriber-management-helper traceoptions]
[edit unified-edge aaa traceoptions]
[edit unified-edge gateways tdf charging traceoptions]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118

Example: Configuring User Permissions with Access Privilege Levels | 124

Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145

Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

trace | 1255
Can view current system-wide, routing table, and protocol-specific values and statistics.

Commands

clear ipv6 router-advertisement
<clear-ipv6-router-advertisement-information>
clear 12circuit auto-sensing
<clear-12ckt-pw-auto-sensing>
clear services redundancy-group
<clear-services-redundancy-group>
clear services redundancy-group statistics
<clear-services-redundancy-group-statistics>
clear services redundancy-set
<clear-services-redundancy-set>
clear services service-sets statistics ids
<clear-service-set-ids-drops-statistics>
clear services traffic-load-balance
<clear-service-traffic-load-balance-statistics>
<request-validation-policy>
show
show access-cac interface-set
<get-access-cac-ifiset>
show access-security
show access-security router-advertisement-guard
show access-security router-advertisement-guard entries
<show-as-router-advetisement-entry>
show access-security router-advertisement-guard state
<show-as-ra-state>
show access-security router-advertisement-guard statistics
<get-as-router-advertisement-statistics>
show access-security router-advertisement-guard statistics interface
<get-as-router-advertisement-interface>
show accounting

show accounting profile
<get-accounting-profile-information>

show accounting records
<get-accounting-record-information>

show amt
show amt statistics
    <get-amt-statistics>
show amt summary
    <get-amt-summary>
show amt tunnel
    <get-amt-tunnel-information>
show amt tunnel gateway-address
    <get-amt-tunnel-gateway-address>
show amt tunnel tunnel-interface
    <get-amt-tunnel-interface>
show analytics collector
    <get-analytics-collector>
show ancp
    show ancp cos
        <get-ancp-cos-information>
show ancp cos last-update
    <get-ancp-cos-last-update-information>

show ancp cos pending-update
    <get-ancp-cos-pending-information>

show ancp neighbor
    <get-ancp-neighbor-information>
show ancp statistics
    <get-ancp-stats-information>
show ancp subscriber
    <get-ancp-subscriber-information>

show ancp subscriber identifier
    <get-ancp-subscriber-identifier-information>
show ancp subscriber ip-address
    <get-ancp-subscriber-ip-address-information>
show ancp subscriber neighbor
    <get-ancp-subscriber-neighbor-information>
show ancp subscriber system-name
    <get-ancp-subscriber-system-name-information>
show ancp subscriber mac-information
    <get-ancp-subscriber-mac-information>
show app-engine
show app-engine information
show app-engine packages
show app-engine packages remote
    <get-virtual-machine-package-remote>
show app-engine packages system
<get-virtual-machine-package-system>
show app-engine processes
show app-engine resource-usage
show app-engine route-table
show app-engine routing-instance
show app-engine routing-instance compute-clusters
show app-engine routing-instance virtual-machines
show app-engine status
show app-engine virtual-machine package
<get-virtual-machine-package-information>
show application-monitor
<get-application-monitor-information>
show application-monitor probe
show application-monitor probe flows
<get-application-monitor-probe-flows-information>
show application-monitor probe measurements
<get-application-monitor-probe-measurements>
show application-monitor probe mirrors
<get-application-monitor-probe-mirrors>
show app-engine virtual-machine vm-instance
show aps
<get-aps-information>

show aps group
<get-aps-group-information>
show aps interface
<get-aps-interface-information>
show arp
<get-arp-table-information>

show as-path
<get-as-path>
show as-path domain
<get-as-path-domain>
show auto-configuration
show auto-configuration interfaces
show backup-selection
<get-backup-selection>
show backup-selection instance
<get-backup-selection-instance>
show bfd
show bfd session
   <get-bfd-session-information>

show bfd session address
   <get-bfd-session-address>
show bfd session client
   <get-bfd-session-client>
show bfd session client rsvp-oam
   <get-bfd-session-client-rsvp>
show bfd session client vpls-oam
   <get-bfd-session-client-vpls>
show bfd session client vpls-oam instance
   <get-bfd-session-client-vpls-instance>
show bfd session discriminator
   <get-bfd-session-discriminator>
show bfd session prefix
   <get-bfd-session-prefix>
show bfd subscriber
show bfd subscriber session
   <get-bfd-subscriber-session>
show bgp
show bgp bmp
   <get-bgp-monitoring-protocol-statistics>
show bgp group
   <get-bgp-group-information>
show bgp group output-queues
   <get-bgp-group-output-queue-information>

show bgp group rtf
   <get-bgp-rtf-information>

show bgp group traffic-statistics
   <get-bgp-traffic-statistics-information>

show bgp neighbor
   <get-bgp-neighbor-information>

show bgp neighbor orf
   <get-bgp-orf-information>
show bgp neighbor output-queue
   <get-bgp-output-queue-information>
show bgp output-scheduler
show bgp replication
<get-bgp-replication-information>
show bgp summary
<get-bgp-summary-information>

show bridge
show bridge domain
<get-bridge-instance-information>

show bridge domain operational
<get-operational-bridge-instance-information>
show bridge domain satellite
<get-satellite-control-bridge-domain>
show bridge evpn
show bridge evpn arp-table
<get-bridge-evpn-arp-table>
show bridge evpn nd-table
<get-bridge-evpn-nd-table>
show bridge evpn peer-gateway-macs
<get-bridge-peer-gateway-mac>
<get-bridge-flood-information>
show bridge flood
show bridge flood event-queue
<get-bridge-domain-event-queue-information>
show bridge flood next-hops
show bridge flood next-hops satellite
<get-satellite-control-composite-next-hop>
show bridge flood route
show bridge flood route all-ce-flood
<get-show-bridge-domain-all-ce-flood-route-information>

show bridge flood route all-ve-flood
<get-show-bridge-domain-ve-flood-route-information>
show bridge flood route alt-root-flood
<get-bridge-domain-alt-root-flood-route-information>
show bridge flood route bd-flood
<get-bridge-domain-bd-flood-route-information>
show bridge flood route mlp-flood
<get-bridge-domain-mlp-flood-route-information>
show bridge flood route re-flood
<get-bridge-domain-re-flood-route-information>
show bridge flood satellite
<get-satellite-control-flood-ethernet>
show bridge interface
show bridge interface satellite
<get-satellite-control-bridge-interface>
show bridge mac-table
  <get-bridge-mac-table>
show bridge mac-table interface
  <get-bridge-interface-mac-table>
show bridge mac-table satellite
<get-satellite-control-bridge-mac-table>
show bridge satellite
show bridge satellite device
<get-satellite-device-db>
show bridge satellite events
<get-satellite-control-history-information>
show bridge satellite logging
<get-satellite-control-logging-information>
show bridge satellite summary
<get-satellite-control-bridge-summary>

show bridge statistics
  <get-bridge-statistics-information>
show chassis
show chassis adc
show chassis alarms
  <get-alarm-information>
show chassis alarms fpc
<get-fpc-alarm-information>
show chassis alarms satellite
<get-chassis-alarm-satellite-information>
show chassis beacon
  get-chassis-beacon-information>
show chassis beacon cb
  <get-chassis-cb-beacon-information>
show chassis environment adc
show chassis environment ccg
<get-environment-ccg-information>
show chassis cfeb
  <get-cfeb-information>
show chassis cip
show chassis craft-interface
<get-craft-information>
show chassis environment
 <get-environment-information>
show chassis environment cb
 <get-environment-cb-information>
show chassis environment cip
 <get-environment-cip-information>
show chassis environment feb
 <get-environment-feb-information>
show chassis environment fan
show chassis environment fpc
 <get-environment-fpc-information>
show chassis environment fpc satellite
 <get-environment-fpc-satellite-info>
show chassis environment fpm
 <get-environment-fpm-information>
show chassis environment mcs
 <get-environment-mcs-information>
show chassis environment pcg
 <get-environment-pcg-information>
show chassis environment pdu
 <get-environment-pdu-information>
show chassis environment pem
 <get-environment-pem-information>
show chassis environment pem satellite
 <get-environment-pem-satellite-info>
show chassis environment psm
show chassis environment psu
 <get-environment-psu-information>
show chassis environment routing-engine
 <get-environment-re-information>
show chassis environment routing-engine satellite
 <get-environment-re-satellite-info>
show chassis environment satellite
 <get-environment-satellite-information>
show chassis environment scg
 <get-environment-scg-information>
show chassis environment service-node
 <get-environment-service-node-information>
show chassis environment sfb
show chassis environment sfm
 <get-environment-sfm-information>
show chassis environment sib
    <get-environment-sib-information>

show chassis environment sib f13
show chassis environment sib f2s
show chassis ethernet-switch
show chassis ethernet-switch errors
show chassis ethernet-switch statistics
show chassis ethernet-switch temperature
show chassis fabric
show chassis fabric degraded-fabric-reachability
show chassis fabric device
    <get-chassis-fabric-information-device>
show chassis fabric connectivity
    <get-chassis-fabric-connectivity-information>
show chassis fabric degradation
    <get-fm-degradation-information>
show chassis fabric degradation actions
    <get-fm-degradation-information-details>
show chassis fabric destinations
    <get-fm-fabric-destinations-state>
show chassis fabric errors
show chassis fabric errors autoheal
    <get-fm-plane-autoheal-errors>
show chassis fabric errors fpc
    <get-fm-fpc-errors>

show chassis fabric errors sib
    <get-fm-sib-errors>

show chassis fabric errors sib f13
show chassis fabric errors sib f2s
show chassis fabric feb
show chassis fabric fpcs
    <get-fm-fpc-state-information>

show chassis fabric links
    <get-chassis-fabric-link-information>
show chassis fabric map
show chassis fabric plane
    <get-fm-plane-state-information>
show chassis fabric plane-location
show chassis fabric reachability
   <get-fm-fabric-reachability-information>
show chassis fabric sibs
   <get-fm-sib-state-information>
show chassis fabric spray-weights
   <get-chassis-fabric-spray-weight-information>
show chassis fabric spray-weights from
show chassis fabric spray-weights to
show chassis fabric summary
   <get-fm-state-information>
show chassis fabric topology
   <get-chassis-fabric-topology-information>
show chassis fabric unreachable-destinations
   <get-fm-unreachable-dest-information>
show chassis fan
show chassis fan satellite
get-chassis-fan-satellite-information
show chassis feb
   <get-feb-brief-information>
show chassis feb detail
   <get-feb-information>
show chassis firmware
   <get-firmware-information>
show chassis firmware detail
   <get-firmware-information-detail>
show chassis firmware satellite
<get-chassis-firmware-satellite-information>
show chassis forwarding
   <get-fwdd-information>
show chassis fpc
   <get-fpc-information>
show chassis fpc errors
   <get-fpc-error-information>
show chassis fpc optical-properties
<get-fpc-optical-information>
show chassis fpc optical-properties alarms
<get-fpc-optical-alarms-information>
show chassis fpc optical-properties amplifier-chain
show chassis fpc optical-properties amplifier-chain ila
<get-fpc-optical-ila-alarms-information>
show chassis fpc optical-properties amplifier-chain ila edfa
<get-fpc-optical-ila-edfa-information>
show chassis fpc optical-properties amplifier-chain ila osc
<get-fpc-optical-ila-osc-information>
show chassis fpc optical-properties amplifier-chain ila pm-current
<get-fpc-optical-ila-pm-current-information>
show chassis fpc optical-properties amplifier-chain ila pm-currentday
<get-fpc-optical-ila-pm-currentday-information>
show chassis fpc optical-properties amplifier-chain ila pm-interval
<get-fpc-optical-ila-pm-interval-information>
show chassis fpc optical-properties amplifier-chain ila pm-previousday
<get-fpc-optical-ila-pm-previousday-information>
show chassis fpc optical-properties amplifier-chain ila summary
<get-fpc-optical-ila-summary-information>
show chassis fpc optical-properties amplifier-chain ila voa
<get-fpc-optical-ila-voa-information>
show chassis fpc optical-properties amplifier-topology
<get-fpc-optical-amplifier-topology-information>
show chassis fpc optical-properties edfa
<get-fpc-optical-edfa-information>
show chassis fpc optical-properties mfg-info
<get-fpc-optical-mfg-info-information>
show chassis fpc optical-properties ocm
<get-fpc-optical-ocm-information>
show chassis fpc optical-properties pm-current
<get-fpc-optical-pm-current-information>
show chassis fpc optical-properties pm-currentday
<get-fpc-optical-pm-currentday-information>
show chassis fpc optical-properties pm-interval
<get-fpc-optical-pm-interval-information>
show chassis fpc optical-properties pm-previousday
<get-fpc-optical-pm-previousday-information>
show chassis fpc optical-properties status
<get-fpc-optical-status-information>
show chassis fpc optical-properties topology
<get-fpc-optical-topology-information>
show chassis fpc optical-properties wss
<get-fpc-optical-wss-information>
show chassis fpc pic-status
<get-pic-information>
show chassis fpc port-status
<get-fpc-port-information>
show chassis fpc-feb-connectivity
<get-fpc-feb-connectivity-information>

show chassis hardware
<get-chassis-inventory>
show chassis hardware satellite
<get-chassis-hardware-satellite-information>
show chassis hss
show chassis hss link-quality
show chassis in-service-upgrade
show chassis ioc-npc-connectivity
<get-ioc-npc-connectivity-information>
show chassis jam-test
<get-jam-test-information>
show chassis lcc-mode
<get-chassis-lcc-mode-information>

show chassis lccs
<get-fru-information>
<get-chassis-led-satellite-information>
show chassis location
<get-chassis-location>

show chassis location fpc
show chassis location interface
show chassis location interface by-name
<get-interface-location-name-information>

show chassis location interface by-slot
<get-interface-location-information>
show chassis mac-addresses
show chassis multicast-loadbalance
<get-chassis-ae-lb-information>
show chassis network-services
  <network-services>
show chassis network-slices
  <get-gnf-information>

show chassis nonstop-upgrade
show chassis pic
  <get-pic-detail>

show chassis power
  <get-power-usage-information>

show chassis power detail
  <get-power-usage-information-detail>
show chassis power sequence
show chassis power upgrade

show chassis power-ratings
  <get-power-management>

show chassis psd
  <get-psd-information>

show chassis redundancy
show chassis redundancy feb
  <get-feb-redundancy-information>

show chassis redundancy feb errors
  <get-feb-redundancy-error-information>

show chassis redundancy feb redundancy-group
  <get-feb-redundancy-group-information>

show chassis redundant-power-system
  <get-rps-chassis-information>

show chassis routing-engine
  <get-route-engine-information>

show chassis routing-engine bios
  <get-bios-version-information>
show chassis routing-engine bios satellite
<get-chassis-routing-engine-bios-satellite-info>
show chassis routing-engine errors
<get-chassis-routing-engine-errors>
show chassis routing-engine satellite
<get-chassis-routing-engine-satellite-information>
show chassis satellite
<get-chassis-satellite-information>
show chassis satellite extended-port
<get-chassis-satellite-extended-port-information>
show chassis satellite interface
<get-chassis-satellite-interface-information>
show chassis satellite neighbor
<get-chassis-satellite-neighbor-information>
show chassis satellite neighbor statistics
<get-chassis-satellite-neighbor-statistics>
show chassis satellite power-budget-statistics
<get-power-budget-information>
show chassis satellite redundancy-group
<get-chassis-satellite-redundancy-group-info>
show chassis satellite redundancy-group devices
<get-chassis-satellite-redundancy-grp-devices-info>
show chassis satellite redundancy-group devices history
<get-chassis-satellite-redundancy-grp-dev-history>
show chassis satellite software
<get-satellite-management-software-information>
show chassis satellite statistics
<get-chassis-satellite-statistics>
show chassis satellite unprovision
<get-chassis-satellite-unprovision-information>
show chassis satellite upgrade-group
<get-chassis-satellite-upgrade-group-information>
show chassis satellite-cluster
<get-chassis-satellite-cluster-information>
show chassis satellite-cluster route
<get-chassis-satellite-cluster-route>
show chassis satellite-cluster statistics
<get-chassis-satellite-cluster-statistics>
show chassis scb
<get-scb-information>

show chassis service-node
<get-service-node-information>
show chassis sfm
   <get-sfm-information>

show chassis sfm detail
show chassis sibs
   <get-sib-information>

show chassis spmb
   <get-spmb-information>
show chassis spmb errors
   <get-spmb-error-information>

show chassis spmb sibs
   <get-spmb-sib-information>

show chassis ssb
   <get-ssb-information>

show chassis synchronization
   <get-clock-synchronization-information>

show chassis synchronization backup
show chassis synchronization gnss
show chassis synchronization master
show chassis system-mode
   <get-system-mode-information>
show chassis temperature-thresholds
   <get-temperature-threshold-information>
show chassis temperature-thresholds satellite
   <get-chassis-temp-thresholds-satellite-info>
show chassis vcpu
show chassis zones
   <get-chassis-zones-information>
show class-of-service
   <get-cos-information>

show class-of-service adaptive-shaper
   <get-cos-adaptive-shaper-information>

show class-of-service application-traffic-control
show class-of-service application-traffic-control counter
show class-of-service application-traffic-control rate-limiters
show class-of-service application-traffic-control rate-limiters rl-all
<get-appqos-swrl-stat-all>
show class-of-service application-traffic-control rate-limiters rl-name
<get-appqos-swrl-stat-name>
show class-of-service application-traffic-control rate-limiters summary
<get-appqos-swrl-stat-summary>
show class-of-service application-traffic-control statistics
show class-of-service application-traffic-control statistics rate-limiter
<get-appqos-rule-statistics>
show class-of-service bind-point
<get-cos-bind-point-feature-information>
show class-of-service bind-point interface
<get-cos-interface-feature-information>
show class-of-service bind-point interface-set
<get-cos-interface-set-feature-information>
show class-of-service bind-point routing-instance
<get-cos-routing-instance-feature-information>
show class-of-service bind-point-ownership
<get-cos-bind-point-ownership-summary>
show class-of-service classifier
<get-cos-classifier-information>
show class-of-service client
show class-of-service client internal-id
<get-cos-junos-client-information>
show class-of-service client name
<get-cos-junos-client-information>
show class-of-service client summary
<get-cos-junos-client-summary>

show class-of-service code-point-aliases
<get-cos-code-point-map-information>

show class-of-service congestion-notification
<get-cos-congestion-notification-information>
show class-of-service drop-profile
<get-cos-drop-profile-information>

show class-of-service fabric
show class-of-service fabric scheduler-map
<get-cos-fabric-scheduler-map-information>
show class-of-service fabric statistics
   <get-fabric-queue-information>

show class-of-service fabric statistics detail
   <get-fabric-queue-detailed-information>

show class-of-service forwarding-class
   <get-cos-forwarding-class-information>

show class-of-service forwarding-class-set
   <get-cos-forwarding-class-set-information>

show class-of-service forwarding-table
   <get-cos-table-information>

show class-of-service forwarding-table classifier
   <get-cos-classifier-table-information>

show class-of-service forwarding-table classifier mapping
   <get-cos-classifier-table-map-information>

show class-of-service forwarding-table drop-profile
   <get-cos-red-information>

show class-of-service forwarding-table fabric
show class-of-service forwarding-table fabric scheduler-map
   <get-cos-fwtab-fabric-scheduler-map-information>

show class-of-service forwarding-table forwarding-class-map
   <get-cos-forwarding-class-map-table-information>

show class-of-service forwarding-table forwarding-class-map mapping
   <get-cos-forwarding-class-map-interface-table-information>

show class-of-service forwarding-table loss-priority-map
   <get-cos-loss-priority-map-table-information>

show class-of-service forwarding-table loss-priority-map mapping
   <get-cos-loss-priority-map-table-binding-information>

show class-of-service forwarding-table loss-priority-rewrite
   <get-cos-loss-priority-rewrite-table-information>
show class-of-service forwarding-table loss-priority-rewrite mapping
   <get-cos-loss-priority-rewrite-table-binding-information>
show class-of-service forwarding-table policer
   <get-cos-policer-table-map-information>
show class-of-service forwarding-table policy-map
   <get-cos-policy-map-table-map-information>
show class-of-service forwarding-table policy-map mapping
   <get-cos-policy-map-table-map-information>
show class-of-service forwarding-table rewrite-rule
   <get-cos-rewrite-table-information>
show class-of-service forwarding-table rewrite-rule mapping
   <get-cos-rewrite-table-map-information>
show class-of-service forwarding-table scheduler-map
   <get-cos-scheduler-map-table-map-information>
show class-of-service forwarding-table scheduler-map mapping
   <get-scheduler-map-table-map-information>
show class-of-service forwarding-table shaper
   <get-cos-shaper-table-map-information>
show class-of-service forwarding-table translation-table
   <get-cos-translation-table-information>
show class-of-service forwarding-table translation-table mapping
   <get-cos-translation-table-mapping-information>
show class-of-service fragmentation-map
   <get-cos-fragmentation-map-information>
show class-of-service interface
   <get-cos-interface-map-information>
show class-of-service interface-set
   <get-cos-interface-set-map-information>
show class-of-service l2tp-session
   <get-cos-l2tp-session-map-information>
show class-of-service loss-priority-map
   <get-cos-loss-priority-map-information>
show class-of-service loss-priority-rewrite
  <get-cos-loss-priority-rewrite-information>
show class-of-service multi-destination
  <get-cos-multi-destination-information>
show class-of-service multi-destination classifier-binding
  <get-cos-multi-destination-classifier-binding-information>

show class-of-service packet-buffer
  <get-cos-packet-buffer-information>
show class-of-service packet-buffer usage
  <get-cos-packet-buffer-usage-information>
show class-of-service policy-map
  <get-cos-policy-map-information>

show class-of-service rewrite-rule
  <get-cos-rewrite-information>

show class-of-service routing-instance
  <get-cos-routing-instance-map-information>

show class-of-service scheduler-hierarchy
show class-of-service scheduler-hierarchy interface
  <get-interface-scheduler-hierarchy-information>

show class-of-service scheduler-hierarchy interface-set
  <get-interface-set-scheduler-hierarchy-information>

show class-of-service scheduler-map
  <get-cos-scheduler-map-information>

show class-of-service traffic-control-profile
  <get-cos-traffic-control-profile-information>

show class-of-service translation-table
  <get-cos-translation-table-map-information>

show class-of-service virtual-channel
  <get-cos-virtual-channel-information>

show class-of-service virtual-channel-group
  <get-cos-virtual-channel-group-information>
show cli
show cli authorization
   <get-authorization-information>
show cli commands
show cli commands
show cli directory
 <get-current-working-directory>
show cli history
show cloud-analytics
show cloud-analytics connections
 <get-cloud-analytics-connections>
show cloud-analytics discovery-service
 <get-cloud-analytics-discovery-service>
show cloud-analytics linecard
 <get-cloud-analytics-lc>
show cloud-analytics resources
 <get-cloud-analytics-resources>
show cloud-analytics resources-sampling
 <get-cloud-analytics-resources-sampling>
show cloud-analytics resources-summary
 <get-cloud-analytics-resources-summary>
show cloud-analytics sensors
 <sensor-information>
show cloud-analytics streaming-policies
 <get-cloud-analytics-streaming-policies>
show configuration
show connections
   <get-ccc-information>
show database-replication
show database-replication statistics
   <get-database-replication-statistics-information>
show database-replication summary
   <get-database-replication-summary-information>
show ddos-protection
show ddos-protection protocols
   <get-ddos-protocols-information>
show ddos-protection protocols all-fiber-channel-enode
   <get-ddos-all-fc-enode-information>
show ddos-protection protocols all-fiber-channel-enode aggregate
   <get-ddos-all-fc-enode-aggregate>
show ddos-protection protocols all-fiber-channel-enode aggregate culprit-flows
<get-ddos-all-fc-enode-aggregate-flows>
show ddos-protection protocols all-fiber-channel-enode culprit-flows
<get-ddos-all-fc-enode-flows>
show ddos-protection protocols all-fiber-channel-enode flow-detection
<get-ddos-all-fc-enode-flow-parameters>
show ddos-protection protocols all-fiber-channel-enode parameters
<get-ddos-all-fc-enode-parameters>
show ddos-protection protocols all-fiber-channel-enode statistics
<get-ddos-all-fc-enode-statistics>
show ddos-protection protocols all-fiber-channel-enode violations
<get-ddos-all-fc-enode-violations>
show ddos-protection protocols amtv4
show ddos-protection protocols amtv4 aggregate
show ddos-protection protocols amtv4 aggregate culprit-flows
show ddos-protection protocols amtv4 culprit-flows
show ddos-protection protocols amtv4 flow-detection
show ddos-protection protocols amtv4 parameters
show ddos-protection protocols amtv4 statistics
show ddos-protection protocols amtv4 violations
show ddos-protection protocols amtv6
show ddos-protection protocols amtv6 aggregate
show ddos-protection protocols amtv6 aggregate culprit-flows
show ddos-protection protocols amtv6 culprit-flows
show ddos-protection protocols amtv6 flow-detection
show ddos-protection protocols amtv6 statistics
show ddos-protection protocols amtv6 violations
show ddos-protection protocols ancp
<get-ddos-ancp-information>
show ddos-protection protocols ancp aggregate
<get-ddos-ancp-aggregate>
show ddos-protection protocols ancp parameters
<get-ddos-ancp-parameters>
show ddos-protection protocols ancp statistics
<get-ddos-ancp-statistics>
show ddos-protection protocols ancp violations
<get-ddos-ancp-violations>
show ddos-protection protocols ancpv6
<get-ddos-ancpv6-information>
show ddos-protection protocols ancpv6 aggregate
get-ddos-ancpv6aggregate
show ddos-protection protocols ancpv6 parameters
get-ddos-ancpv6-parameters
show ddos-protection protocols ancpv6 statistics
get-ddos-ancpv6-statistics
show ddos-protection protocols ancpv6 violations
get-ddos-ancpv6-violations
show ddos-protection protocols arp
get-ddos-arp-information
show ddos-protection protocols arp aggregate
get-ddos-arp-aggregate
show ddos-protection protocols arp parameters
get-ddos-arp-parameters
show ddos-protection protocols arp statistics
get-ddos-arp-statistics
show ddos-protection protocols arp violations
get-ddos-arp-violations
show ddos-protection protocols arp-snoop
<get-ddos-arp-snoop-information>
show ddos-protection protocols arp-snoop aggregate
<get-ddos-arp-snoop-aggregate>
show ddos-protection protocols arp-snoop aggregate culprit-flows
<get-ddos-arp-snoop-aggregate-flows>
show ddos-protection protocols arp-snoop culprit-flows
<get-ddos-arp-snoop-flows>
show ddos-protection protocols arp-snoop flow-detection
<get-ddos-arp-snoop-flow-parameters>
show ddos-protection protocols arp-snoop parameters
<get-ddos-arp-snoop-parameters>
show ddos-protection protocols arp-snoop statistics
<get-ddos-arp-snoop-statistics>
show ddos-protection protocols arp-snoop violations
<get-ddos-arp-snoop-violations>
show ddos-protection protocols atm
get-ddos-atm-information
show ddos-protection protocols atm aggregate
get-ddos-atm-aggregate
show ddos-protection protocols atm parameters
get-ddos-atm-parameters
show ddos-protection protocols atm statistics
get-ddos-atm-statistics
show ddos-protection protocols atm violations
get-ddos-atm-violations
show ddos-protection protocols bfd
get-ddos-bfd-information
show ddos-protection protocols bfd aggregate
get-ddos-bfd-aggregate
show ddos-protection protocols bfd parameters
get-ddos-bfd-parameters
show ddos-protection protocols bfd statistics
get-ddos-bfd-statistics
show ddos-protection protocols bfd violations
get-ddos-bfd-violations
show ddos-protection protocols bfdv6
get-ddos-bfdv6-information
show ddos-protection protocols bfdv6 aggregate
get-ddos-bfdv6-aggregate
show ddos-protection protocols bfdv6 parameters
get-ddos-bfdv6-parameters
show ddos-protection protocols bfdv6 statistics
get-ddos-bfdv6-statistics
show ddos-protection protocols bfdv6 violations
get-ddos-bfdv6-violations
show ddos-protection protocols bgp
get-ddos-bgp-information
show ddos-protection protocols bgp aggregate
get-ddos-bgp-aggregate
show ddos-protection protocols bgp parameters
get-ddos-bgp-parameters
show ddos-protection protocols bgp statistics
get-ddos-bgp-statistics
show ddos-protection protocols bgp violations
get-ddos-bgp-violations
show ddos-protection protocols bgpv6
get-ddos-bgpv6-information
show ddos-protection protocols bgpv6 aggregate
get-ddos-bgpv6-aggregate
show ddos-protection protocols bgpv6 parameters
get-ddos-bgpv6-parameters
show ddos-protection protocols bgpv6 statistics
get-ddos-bgpv6-statistics
show ddos-protection protocols bgpv6 violations
get-ddos-bgpv6-violations
show ddos-protection protocols bridge-control
<get-ddos-brg-ctrl-information>
show ddos-protection protocols bridge-control aggregate
<get-ddos-brg-ctrl-aggregate>
show ddos-protection protocols bridge-control aggregate culprit-flows
<get-ddos-brg-ctrl-aggregate-flows>
show ddos-protection protocols bridge-control culprit-flows
<get-ddos-brg-ctrl-flows>
show ddos-protection protocols bridge-control flow-detection
<get-ddos-brg-ctrl-flow-parameters>
show ddos-protection protocols bridge-control parameters
<get-ddos-brg-ctrl-parameters>
show ddos-protection protocols bridge-control statistics
<get-ddos-brg-ctrl-statistics>
show ddos-protection protocols bridge-control violations
<get-ddos-brg-ctrl-violations>
show ddos-protection protocols demux-autosense
get-ddos-demuxauto-information
show ddos-protection protocols demux-autosense aggregate
<get-ddos-demuxauto-aggregate>
show ddos-protection protocols demux-autosense parameters
<get-ddos-demuxauto-parameters>
show ddos-protection protocols demux-autosense statistics
<get-ddos-demuxauto-statistics>
show ddos-protection protocols demux-autosense violations
<get-ddos-demuxauto-violations>
show ddos-protection protocols dhcpv4
get-ddos-dhcpv4-information
show ddos-protection protocols dhcpv4 ack
<get-ddos-dhcpv4-ack>
show ddos-protection protocols dhcpv4 aggregate
<get-ddos-dhcpv4-aggregate>
show ddos-protection protocols dhcpv4 bad-packets
<get-ddos-dhcpv4-bad-pack>
show ddos-protection protocols dhcpv4 bootp
<get-ddos-dhcpv4-bootp>
show ddos-protection protocols dhcpv4 decline
<get-ddos-dhcpv4-decline>
show ddos-protection protocols dhcpv4 discover
<get-ddos-dhcpv4-discover>
show ddos-protection protocols dhcpv4 force-renew
get-ddos-dhcpv4-forcerenew
show ddos-protection protocols dhcpv4 inform
get-ddos-dhcpv4-inform
show ddos-protection protocols dhcpv4 lease-active
get-ddos-dhcpv4-leaseact
show ddos-protection protocols dhcpv4 lease-query
get-ddos-dhcpv4-leasequery
show ddos-protection protocols dhcpv4 lease-unassigned
get-ddos-dhcpv4-leaseuna
show ddos-protection protocols dhcpv4 lease-unknown
get-ddos-dhcpv4-leaseunk
show ddos-protection protocols dhcpv4 nak
get-ddos-dhcpv4-nak
show ddos-protection protocols dhcpv4 no-message-type
get-ddos-dhcpv4-no-mstype
show ddos-protection protocols dhcpv4 offer
get-ddos-dhcpv4-offer
show ddos-protection protocols dhcpv4 offer culprit-flows
show ddos-protection protocols dhcpv4 parameters
get-ddos-dhcpv4-parameters
show ddos-protection protocols dhcpv4 release
get-ddos-dhcpv4-release
show ddos-protection protocols dhcpv4 renew
get-ddos-dhcpv4-renew
show ddos-protection protocols dhcpv4 request
get-ddos-dhcpv4-request
show ddos-protection protocols dhcpv4 statistics
get-ddos-dhcpv4-statistics
show ddos-protection protocols dhcpv4 unclassified
get-ddos-dhcpv4-unclass
show ddos-protection protocols dhcpv4 violations
get-ddos-dhcpv4-violations
show ddos-protection protocols dhcpv4v6
<get-ddos-dhcpv4v6-information>
show ddos-protection protocols dhcpv4v6 aggregate
<get-ddos-dhcpv4v6-aggregate>
show ddos-protection protocols dhcpv4v6 aggregate culprit-flows
<get-ddos-dhcpv4v6-aggregate-flows>
show ddos-protection protocols dhcpv4v6 culprit-flows
<get-ddos-dhcpv4v6-flows>
show ddos-protection protocols dhcpv4v6 flow-detection
<get-ddos-dhcpv4v6-flow-parameters>
show ddos-protection protocols dhcpv4v6 parameters
<get-ddos-dhcpv4v6-parameters>
show ddos-protection protocols dhcpv4v6 statistics
<get-ddos-dhcpv4v6-statistics>
show ddos-protection protocols dhcpv4v6 violations
<get-ddos-dhcpv4v6-violations>
show ddos-protection protocols dhcpv6
get-ddos-dhcpv6-information
show ddos-protection protocols dhcpv6 advertise
get-ddos-dhcpv6-advertise
show ddos-protection protocols dhcpv6 advertise culprit-flows
show ddos-protection protocols dhcpv6 aggregate
get-ddos-dhcpv6-aggregate
show ddos-protection protocols dhcpv6 confirm
get-ddos-dhcpv6-confirm
show ddos-protection protocols dhcpv6 decline
get-ddos-dhcpv6-decline
show ddos-protection protocols dhcpv6 information-request
get-ddos-dhcpv6-info-req
show ddos-protection protocols dhcpv6 leasequery
get-ddos-dhcpv6-leasequery
show ddos-protection protocols dhcpv6 leasequery culprit-flows
show ddos-protection protocols dhcpv6 leasequery-data
get-ddos-dhcpv6-leaseq-da
show ddos-protection protocols dhcpv6 leasequery-done
get-ddos-dhcpv6-leaseq-do
show ddos-protection protocols dhcpv6 leasequery-reply
get-ddos-dhcpv6-leaseq-re
show ddos-protection protocols dhcpv6 parameters
get-ddos-dhcpv6-parameters
show ddos-protection protocols dhcpv6 rebind
get-ddos-dhcpv6-rebind
show ddos-protection protocols dhcpv6 reconfigure
get-ddos-dhcpv6-reconfig
show ddos-protection protocols dhcpv6 relay-forward
get-ddos-dhcpv6-relay-for
show ddos-protection protocols dhcpv6 relay-reply
get-ddos-dhcpv6-relay-rep
show ddos-protection protocols dhcpv6 release
get-ddos-dhcpv6-release
show ddos-protection protocols dhcpv6 renew
get-ddos-dhcpv6-renew
show ddos-protection protocols dhcpv6 reply
get-ddos-dhcpv6-reply
show ddos-protection protocols dhcpv6 request
get-ddos-dhcpv6-request
show ddos-protection protocols dhcpv6 solicit
get-ddos-dhcpv6-solicit
show ddos-protection protocols dhcpv6 statistics
get-ddos-dhcpv6-statistics
show ddos-protection protocols dhcpv6 unclassified
get-ddos-dhcpv6-unclass
show ddos-protection protocols dhcpv6 unclassified culprit-flows
get-ddos-dhcpv6-violations
show ddos-protection protocols diameter
get-ddos-diameter-information
show ddos-protection protocols diameter aggregate
get-ddos-diameter-aggregate
show ddos-protection protocols diameter parameters
get-ddos-diameter-parameters
show ddos-protection protocols diameter statistics
get-ddos-diameter-statistics
show ddos-protection protocols diameter violations
get-ddos-diameter-violations
show ddos-protection protocols dns
get-ddos-dns-information
show ddos-protection protocols dns aggregate
get-ddos-dns-aggregate
show ddos-protection protocols dns parameters
get-ddos-dns-parameters
show ddos-protection protocols dns statistics
get-ddos-dns-statistics
show ddos-protection protocols dns violations
get-ddos-dns-violations
show ddos-protection protocols dtcp
get-ddos-dtcp-information
show ddos-protection protocols dtcp aggregate
get-ddos-dtcp-aggregate
show ddos-protection protocols dtcp aggregate culprit-flows
get-ddos-dtcp-violations
show ddos-protection protocols dtcp parameters
get-ddos-dtcp-parameters
show ddos-protection protocols dtcp statistics
get-ddos-dtcp-statistics
show ddoos-protection protocols dtcp violations
get-ddos-dtcp-violations
show ddoos-protection protocols dynamic-vlan
get-ddos-dynvlan-information
show ddoos-protection protocols dynamic-vlan aggregate
get-ddos-dynvlan-aggregate
show ddoos-protection protocols dynamic-vlan parameters
get-ddos-dynvlan-parameters
show ddoos-protection protocols dynamic-vlan statistics
get-ddos-dynvlan-statistics
show ddoos-protection protocols dynamic-vlan violations
get-ddos-dynvlan-violations
show ddoos-protection protocols egpv6
get-ddos-egpv6-information
show ddoos-protection protocols egpv6 aggregate
get-ddos-egpv6-aggregate
show ddoos-protection protocols egpv6 parameters
get-ddos-egpv6-parameters
show ddoos-protection protocols egpv6 statistics
get-ddos-egpv6-statistics
show ddoos-protection protocols egpv6 violations
get-ddos-egpv6-violations
show ddoos-protection protocols eoam
get-ddos-eoam-information
show ddoos-protection protocols eoam aggregate
get-ddos-eoam-aggregate
show ddoos-protection protocols eoam parameters
get-ddos-eoam-parameters
show ddoos-protection protocols eoam statistics
get-ddos-eoam-statistics
show ddoos-protection protocols eoam violations
get-ddos-eoam-violations
show ddoos-protection protocols esmc
get-ddos-esmc-information
show ddoos-protection protocols esmc aggregate
get-ddos-esmc-aggregate
show ddoos-protection protocols esmc parameters
get-ddos-esmc-parameters
show ddoos-protection protocols esmc statistics
get-ddos-esmc-statistics
show ddoos-protection protocols esmc violations
get-ddos-esmc-violations
show ddos-protection protocols ethernet-tcc
<get-ddos-eth-tcc-information>
show ddos-protection protocols ethernet-tcc aggregate
<get-ddos-eth-tcc-aggregate>
show ddos-protection protocols ethernet-tcc aggregate culprit-flows
<get-ddos-eth-tcc-aggregate-flows>
show ddos-protection protocols ethernet-tcc culprit-flows
<get-ddos-eth-tcc-flows>
show ddos-protection protocols ethernet-tcc flow-detection
<get-ddos-eth-tcc-flow-parameters>
show ddos-protection protocols ethernet-tcc parameters
<get-ddos-eth-tcc-parameters>
show ddos-protection protocols ethernet-tcc statistics
<get-ddos-eth-tcc-statistics>
show ddos-protection protocols ethernet-tcc violations
<get-ddos-eth-tcc-violations>
show ddos-protection protocols exceptions
<get-ddos-exception-information>
show ddos-protection protocols exceptions aggregate
<get-ddos-exception-aggregate>
show ddos-protection protocols exceptions aggregate culprit-flows
<get-ddos-exception-aggregate-flows>
show ddos-protection protocols exceptions culprit-flows
<get-ddos-exception-flows>
show ddos-protection protocols exceptions flow-detection
<get-ddos-exception-flow-parameters>
show ddos-protection protocols exceptions mcast-rpf-err
<get-ddos-exception-mcast-rpf>
show ddos-protection protocols exceptions mcast-rpf-err culprit-flows
<get-ddos-exception-mcast-rpf-flows>
show ddos-protection protocols exceptions mtu-exceeded
<get-ddos-exception-mtu-exceed>
show ddos-protection protocols exceptions mtu-exceeded culprit-flows
<get-ddos-exception-mtu-exceed-flows>
show ddos-protection protocols exceptions parameters
<get-ddos-exception-parameters>
show ddos-protection protocols exceptions statistics
<get-ddos-exception-statistics>
show ddos-protection protocols exceptions unclassified
<get-ddos-exception-unclass>
show ddos-protection protocols exceptions unclassified culprit-flows
<get-ddos-exception-unclass-flows>
show ddos-protection protocols exceptions violations
<get-ddos-exception-violations>

show ddos-protection protocols fab-probe
<get-ddos-fab-probe-information>
show ddos-protection protocols fab-probe aggregate
<get-ddos-fab-probe-aggregate>
show ddos-protection protocols fab-probe parameters
<get-ddos-fab-probe-parameters>
show ddos-protection protocols fab-probe statistics
<get-ddos-fab-probe-statistics>
show ddos-protection protocols fab-probe violations
<get-ddos-fab-probe-violations>
show ddos-protection protocols firewall-host
   get-ddos-fw-host-information
show ddos-protection protocols firewall-host aggregate
   get-ddos-fw-host-aggregate
show ddos-protection protocols firewall-host parameters
   get-ddos-fw-host-parameters
show ddos-protection protocols firewall-host statistics
   get-ddos-fw-host-statistics
show ddos-protection protocols firewall-host violations
   get-ddos-fw-host-violations

show ddos-protection protocols ftp
   get-ddos-ftp-information
show ddos-protection protocols ftp aggregate
   get-ddos-ftp-aggregate
show ddos-protection protocols ftp parameters
   get-ddos-ftp-parameters
show ddos-protection protocols ftp statistics
   get-ddos-ftp-statistics
show ddos-protection protocols ftp violations
   get-ddos-ftp-violations
show ddos-protection protocols ftpv6
   get-ddos-ftpv6-information
show ddos-protection protocols ftpv6 aggregate
   get-ddos-ftpv6-aggregate
show ddos-protection protocols ftpv6 parameters
   get-ddos-ftpv6-parameters
show ddos-protection protocols ftpv6 statistics
get-ddos-ftpv6-statistics
show ddos-protection protocols ftpv6 violations
get-ddos-ftpv6-violations
show ddos-protection protocols garp-reply
<get-ddos-garp-reply-information>
show ddos-protection protocols garp-reply aggregate
<get-ddos-garp-reply-aggregate>
show ddos-protection protocols garp-reply aggregate culprit-flows
<get-ddos-garp-reply-aggregate-flows>
show ddos-protection protocols garp-reply culprit-flows
<get-ddos-garp-reply-flows>
show ddos-protection protocols garp-reply flow-detection
<get-ddos-garp-reply-flow-detection>
show ddos-protection protocols garp-reply parameters
<get-ddos-garp-reply-parameters>
show ddos-protection protocols garp-reply statistics
<get-ddos-garp-reply-statistics>
show ddos-protection protocols garp-reply violations
<get-ddos-garp-reply-violations>
show ddos-protection protocols gre
get-ddos-gre-information
show ddos-protection protocols gre aggregate
get-ddos-gre-aggregate
show ddos-protection protocols gre hbc
<get-ddos-gre-hbc>
show ddos-protection protocols gre hbc culprit-flows
<get-ddos-gre-hbc-flows>
show ddos-protection protocols gre parameters
<get-ddos-gre-parameters>
show ddos-protection protocols gre punt
<get-ddos-gre-punt>
show ddos-protection protocols gre punt culprit-flows
<get-ddos-gre-punt-flows>
show ddos-protection protocols gre statistics
<get-ddos-gre-statistics>
show ddos-protection protocols gre violations
<get-ddos-gre-violations>
show ddos-protection protocols icmp
<get-ddos-icmp-information>
show ddos-protection protocols icmp aggregate
<get-ddos-icmp-aggregate>
show ddos-protection protocols icmp parameters
get-ddos-icmp-parameters
get-ddos-icmp-v6
show ddos-protection protocols icmp statistics
get-ddos-icmp-statistics
show ddos-protection protocols icmp violations
get-ddos-icmp-violations
show ddos-protection protocols icmpv6
<get-ddos-icmpv6-information>
show ddos-protection protocols icmpv6 aggregate
<get-ddos-icmpv6-aggregate>
show ddos-protection protocols icmpv6 aggregate culprit-flows
<get-ddos-icmpv6-aggregate-flows>
show ddos-protection protocols icmpv6 parameters
<get-ddos-icmpv6-parameters>
show ddos-protection protocols icmpv6 statistics
<get-ddos-icmpv6-statistics>
show ddos-protection protocols icmpv6 violations
<get-ddos-icmpv6-violations>
show ddos-protection protocols igmp
get-ddos-igmp-information
show ddos-protection protocols igmp aggregate
get-ddos-igmp-aggregate
show ddos-protection protocols igmp aggregate culprit-flows
show ddos-protection protocols igmp parameters
get-ddos-igmp-parameters
show ddos-protection protocols igmp statistics
<get-ddos-igmp-statistics>
show ddos-protection protocols igmp violations
<get-ddos-igmp-violations>
show ddos-protection protocols igmp-snoop
get-ddos-igmp-snoop-information
show ddos-protection protocols igmp-snoop aggregate
<get-ddos-igmp-snoop-aggregate>
show ddos-protection protocols igmp-snoop parameters
<get-ddos-igmp-snoop-parameters>
show ddos-protection protocols igmp-snoop statistics
<get-ddos-igmp-snoop-statistics>
show ddos-protection protocols igmp-snoop violations
<get-ddos-igmp-snoop-violations>
show ddos-protection protocols igmpv4v6
get-ddos-igmpv4v6-information
show ddos-protection protocols igmpv4v6 aggregate
<get-ddos-igmpv4v6-aggregate>
show ddos-protection protocols igmpv4v6 aggregate culprit-flows
get-ddos-igmpv4v6-parameters
get-ddos-igmpv4v6-statistics
get-ddos-igmpv4v6-violations
get-ddos-igmpv4v6-violations
get-ddos-igmpv6-information
get-ddos-igmpv6-aggregate
get-ddos-igmpv6-aggregate
get-ddos-igmpv6-parameters
get-ddos-igmpv6-statistics
get-ddos-igmpv6-violations
get-ddos-igmpv6-violations
get-ddos-ip-frag-information
get-ddos-ip-frag-aggregate
get-ddos-ip-frag-aggregate
get-ddos-ip-frag-first-frag
get-ddos-ip-frag-parameters
get-ddos-ip-frag-parameters
get-ddos-ip-frag-parameters
get-ddos-ip-frag-first-frag
get-ddos-ip-frag-first-frag
get-ddos-ip-frag-statistics
get-ddos-ip-frag-statistics
get-ddos-ip-frag-trail-frag
get-ddos-ip-frag-trail-frag
get-ddos-ip-frag-violations
get-ddos-ip-frag-violations
get-ddos-ip-opt-information
get-ddos-ip-opt-parameters
get-ddos-ip-opt-parameters
get-ddos-ip-opt-router-alert
get-ddos-ip-opt-router-alert
get-ddos-ip-opt-violations
get-ddos-ip-opt-violations
get-ddos-ip-opt-violations
get-ddos-ip-opt-violations
get-ddos-ip-opt-statistics
show ddos-protection protocols ip-options unclassified
get-ddos-ip-opt-unclass
show ddos-protection protocols ipmc-reserved culprit-flows
<get-ddos-ipmc-reserved-flows>
show ddos-protection protocols ipmc-reserved flow-detection
<get-ddos-ipmc-reserved-flow-parameters>
show ddos-protection protocols ipmc-reserved parameters
<get-ddos-ipmc-reserved-parameters>
show ddos-protection protocols ipmc-reserved statistics
<get-ddos-ipmc-reserved-statistics>
show ddos-protection protocols ipmc-reserved violations
<get-ddos-ipmc-reserved-violations>
show ddos-protection protocols ipmcast-miss
<get-ddos-ipmcast-miss-information>
show ddos-protection protocols ipmcast-miss aggregate
<get-ddos-ipmcast-miss-aggregate>
show ddos-protection protocols ipmcast-miss aggregate culprit-flows
<get-ddos-ipmcast-miss-aggregate-flows>
show ddos-protection protocols ipmcast-miss culprit-flows
<get-ddos-ipmcast-miss-flows>
show ddos-protection protocols ipmcast-miss flow-detection
<get-ddos-ipmcast-miss-flow-parameters>
show ddos-protection protocols ipmcast-miss parameters
<get-ddos-ipmcast-miss-parameters>
show ddos-protection protocols ipmcast-miss statistics
<get-ddos-ipmcast-miss-statistics>
show ddos-protection protocols ipmcast-miss violations
<get-ddos-ipmcast-miss-violations>
show ddos-protection protocols ip-options violations
get-ddos-ip-opt-violations
show ddos-protection protocols ipv4-unclassified
get-ddos-ipv4-uncls-information
show ddos-protection protocols ipv4-unclassified aggregate
get-ddos-ipv4-uncls-aggregate
show ddos-protection protocols ipv4-unclassified parameters
get-ddos-ipv4-uncls-parameters
show ddos-protection protocols ipv4-unclassified statistics
get-ddos-ipv4-uncls-statistics
show ddos-protection protocols ipv4-unclassified violations
get-ddos-ipv4-uncls-violations
show ddos-protection protocols ipv6-unclassified
get-ddos-ipv6-uncls-information
show ddos-protection protocols ipv6-unclassified aggregate
get-ddos-ipv6-uncls-aggregate
show ddos-protection protocols ipv6-unclassified parameters
get-ddos-ipv6-uncls-parameters
show ddos-protection protocols ipv6-unclassified statistics
get-ddos-ipv6-uncls-statistics
show ddos-protection protocols ipv6-unclassified violations
get-ddos-ipv6-uncls-violations
show ddos-protection protocols isis
get-ddos-isis-information
show ddos-protection protocols isis aggregate
get-ddos-isis-aggregate
show ddos-protection protocols isis parameters
get-ddos-isis-parameters
show ddos-protection protocols isis statistics
get-ddos-isis-statistics
show ddos-protection protocols isis violations
get-ddos-isis-violations
show ddos-protection protocols iso-tcc
<get-ddos-iso-tcc-information>
show ddos-protection protocols iso-tcc aggregate
<get-ddos-iso-tcc-aggregate>
show ddos-protection protocols iso-tcc aggregate culprit-flows
<get-ddos-iso-tcc-aggregate-flows>
show ddos-protection protocols iso-tcc culprit-flows
<get-ddos-iso-tcc-flows>
show ddos-protection protocols iso-tcc flow-detection
<get-ddos-iso-tcc-flow-parameters>
show ddos-protection protocols iso-tcc parameters
<get-ddos-iso-tcc-parameters>
show ddos-protection protocols iso-tcc statistics
<get-ddos-iso-tcc-statistics>
show ddos-protection protocols iso-tcc violations
<get-ddos-iso-tcc-violations>
show ddos-protection protocols jfm
get-ddos-jfm-information
show ddos-protection protocols jfm aggregate
get-ddos-jfm-aggregate
show ddos-protection protocols jfm parameters
get-ddos-jfm-parameters
show ddos-protection protocols jfm statistics
get-ddos-jfm-statistics
show ddos-protection protocols jfm violations
get-ddos-jfm-violations
show ddos-protection protocols 12tp
get-ddos-12tp-information
show ddos-protection protocols 12tp aggregate
get-ddos-12tp-aggregate
show ddos-protection protocols 12tp parameters
get-ddos-12tp-parameters
show ddos-protection protocols 12tp statistics
get-ddos-12tp-statistics
show ddos-protection protocols 12tp violations
get-ddos-12tp-violations
show ddos-protection protocols 13dest-miss
<get-ddos-13dest-miss-information>
show ddos-protection protocols 13dest-miss aggregate
<get-ddos-13dest-miss-aggregate>
show ddos-protection protocols 13dest-miss aggregate culprit-flows
<get-ddos-13dest-miss-aggregate-flows>
show ddos-protection protocols 13dest-miss culprit-flows
<get-ddos-13dest-miss-flows>
show ddos-protection protocols 13dest-miss flow-detection
<get-ddos-13dest-miss-flow-parameters>
show ddos-protection protocols 13dest-miss parameters
<get-ddos-13dest-miss-parameters>
show ddos-protection protocols 13dest-miss statistics
<get-ddos-13dest-miss-statistics>
show ddos-protection protocols 13dest-miss violations
<get-ddos-13dest-miss-violations>
show ddos-protection protocols 13mc-sgv-hit-icl
<get-ddos-13mc-sgv-hit-icl-information>
show ddos-protection protocols 13mc-sgv-hit-icl aggregate
<get-ddos-13mc-sgv-hit-icl-aggregate>
show ddos-protection protocols 13mc-sgv-hit-icl aggregate culprit-flows
<get-ddos-13mc-sgv-hit-icl-aggregate-flows>
show ddos-protection protocols 13mc-sgv-hit-icl culprit-flows
<get-ddos-13mc-sgv-hit-icl-flows>
show ddos-protection protocols 13mc-sgv-hit-icl flow-detection
<get-ddos-13mc-sgv-hit-icl-flow-parameters>
show ddos-protection protocols 13mc-sgv-hit-icl parameters
<get-ddos-13mc-sgv-hit-icl-parameters>
show ddos-protection protocols 13mc-sgv-hit-icl statistics
<get-ddos-l3mc-sgv-hit-icl-statistics>
show ddos-protection protocols l3mc-sgv-hit-icl violations
<get-ddos-l3mc-sgv-hit-icl-violations>
show ddos-protection protocols l3mtu-fail
<get-ddos-l3mtu-fail-information>
show ddos-protection protocols l3mtu-fail aggregate
<get-ddos-l3mtu-fail-aggregate>
show ddos-protection protocols l3mtu-fail aggregate culprit-flows
<get-ddos-l3mtu-fail-aggregate-flows>
show ddos-protection protocols l3mtu-fail culprit-flows
<get-ddos-l3mtu-fail-flows>
show ddos-protection protocols l3mtu-fail flow-detection
<get-ddos-l3mtu-fail-flow-parameters>
show ddos-protection protocols l3mtu-fail parameters
<get-ddos-l3mtu-fail-parameters>
show ddos-protection protocols l3mtu-fail statistics
<get-ddos-l3mtu-fail-statistics>
show ddos-protection protocols l3mtu-fail violations
<get-ddos-l3mtu-fail-violations>
show ddos-protection protocols l3nhop
<get-ddos-l3nhop-information>
show ddos-protection protocols l3nhop aggregate
<get-ddos-l3nhop-aggregate>
show ddos-protection protocols l3nhop aggregate culprit-flows
<get-ddos-l3nhop-aggregate-flows>
show ddos-protection protocols l3nhop culprit-flows
<get-ddos-l3nhop-flows>
show ddos-protection protocols l3nhop flow-detection
<get-ddos-l3nhop-flow-parameters>
show ddos-protection protocols l3nhop parameters
<get-ddos-l3nhop-parameters>
show ddos-protection protocols l3nhop statistics
<get-ddos-l3nhop-statistics>
show ddos-protection protocols l3nhop violations
<get-ddos-l3nhop-violations>
show ddos-protection protocols lacp
<get-ddos-lacp-information>
show ddos-protection protocols lacp aggregate
<get-ddos-lacp-aggregate>
show ddos-protection protocols lacp parameters
<get-ddos-lacp-parameters>
show ddos-protection protocols lacp statistics
<get-ddos-lacp-statistics>
show ddos-protection protocols lacp violations
<get-ddos-lacp-violations>
show ddos-protection protocols ldp
<get-ddos-ldp-information>
show ddos-protection protocols ldp aggregate
<get-ddos-ldp-aggregate>
show ddos-protection protocols ldp parameters
<get-ddos-ldp-parameters>
show ddos-protection protocols ldp statistics
<get-ddos-ldp-statistics>
show ddos-protection protocols ldp violations
<get-ddos-ldp-violations>
show ddos-protection protocols ldp-hello
<get-ddos-ldp-hello-information>
show ddos-protection protocols ldp-hello aggregate
<get-ddos-ldp-hello-aggregate>
show ddos-protection protocols ldp-hello aggregate culprit-flows
<get-ddos-ldp-hello-aggregate-flows>
show ddos-protection protocols ldp-hello culprit-flows
<get-ddos-ldp-hello-flows>
show ddos-protection protocols ldp-hello flow-detection
<get-ddos-ldp-hello-flow-parameters>
show ddos-protection protocols ldp-hello parameters
<get-ddos-ldp-hello-parameters>
show ddos-protection protocols ldp-hello statistics
<get-ddos-ldp-hello-statistics>
show ddos-protection protocols ldp-hello violations
<get-ddos-ldp-hello-violations>
show ddos-protection protocols ldpv6
<get-ddos-ldp6-information>
show ddos-protection protocols ldpv6 aggregate
<get-ddos-ldp6-aggregate>
show ddos-protection protocols ldpv6 parameters
<get-ddos-ldp6-parameters>
show ddos-protection protocols ldpv6 statistics
<get-ddos-ldp6-statistics>
show ddos-protection protocols ldpv6 violations
<get-ddos-ldp6-violations>
show ddos-protection protocols lldp
<get-ddos-lldp-information>
show ddos-protection protocols lldp aggregate
<get-ddos-lldp-aggregate>
show ddos-protection protocols lldp parameters
<get-ddos-lldp-parameters>
show ddos-protection protocols lldp statistics
<get-ddos-lldp-statistics>
show ddos-protection protocols lldp violations
<get-ddos-lldp-violations>
show ddos-protection protocols lmp
<get-ddos-lmp-information>
show ddos-protection protocols lmp aggregate
<get-ddos-lmp-aggregate>
show ddos-protection protocols lmp parameters
<get-ddos-lmp-parameters>
show ddos-protection protocols lmp statistics
<get-ddos-lmp-statistics>
show ddos-protection protocols lmp violations
<get-ddos-lmp-violations>
show ddos-protection protocols lmpv6
<get-ddos-lmpv6-information>
show ddos-protection protocols lmpv6 aggregate
<get-ddos-lmpv6-aggregate>
show ddos-protection protocols lmpv6 parameters
<get-ddos-lmpv6-parameters>
show ddos-protection protocols lmpv6 statistics
<get-ddos-lmpv6-statistics>
show ddos-protection protocols lmpv6 violations
<get-ddos-lmpv6-violations>
show ddos-protection protocols localnh
<get-ddos-localnh-information>
show ddos-protection protocols localnh aggregate
<get-ddos-localnh-aggregate>
show ddos-protection protocols localnh aggregate culprit-flows
<get-ddos-localnh-aggregate-flows>
show ddos-protection protocols localnh culprit-flows
<get-ddos-localnh-flows>
show ddos-protection protocols localnh flow-detection
<get-ddos-localnh-flow-parameters>
show ddos-protection protocols localnh parameters
<get-ddos-localnh-parameters>
show ddos-protection protocols localnh statistics
<get-ddos-localnh-statistics>
show ddos-protection protocols localnh violations
<get-ddos-localnh-violations>
show ddos-protection protocols mac-host
<get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
<get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host aggregate culprit-flows
<get-ddos-mac-host-aggregate-flows>
show ddos-protection protocols mac-host culprit-flows
<get-ddos-mac-host-flows>
show ddos-protection protocols mac-host flow-detection
<get-ddos-mac-host-flow-parameters>
show ddos-protection protocols mac-host parameters
<get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
<get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
<get-ddos-mac-host-violations>
show ddos-protection protocols martian-address
<get-ddos-martian-address-information>
show ddos-protection protocols martian-address aggregate
<get-ddos-martian-address-aggregate>
show ddos-protection protocols martian-address aggregate culprit-flows
<get-ddos-martian-address-aggregate-flows>
show ddos-protection protocols martian-address culprit-flows
<get-ddos-martian-address-flows>
show ddos-protection protocols martian-address flow-detection
<get-ddos-martian-address-flow-parameters>
show ddos-protection protocols martian-address parameters
<get-ddos-martian-address-parameters>
show ddos-protection protocols martian-address statistics
<get-ddos-martian-address-statistics>
show ddos-protection protocols martian-address violations
<get-ddos-martian-address-violations>
show ddos-protection protocols mac-host
<get-ddos-mac-host-information>
show ddos-protection protocols mac-host aggregate
<get-ddos-mac-host-aggregate>
show ddos-protection protocols mac-host parameters
<get-ddos-mac-host-parameters>
show ddos-protection protocols mac-host statistics
<get-ddos-mac-host-statistics>
show ddos-protection protocols mac-host violations
<get-ddos-mac-host-violations>
show ddos-protection protocols mcast-snoop mld
<get-ddos-mcast-snoop-mld>
show ddos-protection protocols mcast-snoop mld culprit-flows
<get-ddos-mcast-snoop-mld-flows>
show ddos-protection protocols mld
<get-ddos-mld-information>
show ddos-protection protocols mld aggregate
<get-ddos-mld-aggregate>
show ddos-protection protocols mld aggregate culprit-flows
show ddos-protection protocols mld culprit-flows
<get-ddos-mld-flows>
show ddos-protection protocols mld flow-detection
<get-ddos-mld-flow-parameters>
show ddos-protection protocols mld parameters
<get-ddos-mld-parameters>
show ddos-protection protocols mld statistics
<get-ddos-mld-statistics>
show ddos-protection protocols mld violations
<get-ddos-mld-violations>
show ddos-protection protocols mlp
<get-ddos-mlp-information>
show ddos-protection protocols mlp add
<get-ddos-mlp-add>
show ddos-protection protocols mlp add culprit-flows
<get-ddos-mlp-add-flows>
show ddos-protection protocols mlp aggregate
<get-ddos-mlp-aggregate>
show ddos-protection protocols mlp aggregate culprit-flows
<get-ddos-mlp-aggregate-flows>
show ddos-protection protocols mlp culprit-flows
<get-ddos-mlp-flows>
show ddos-protection protocols mlp delete
<get-ddos-mlp-delete>
show ddos-protection protocols mlp delete culprit-flows
get-ddos-mlp-delete-flows
show ddos-protection protocols mlp flow-detection
get-ddos-mlp-flow-parameters
show ddos-protection protocols mlp lookup
<get-ddos-mlp-lookup>
show ddos-protection protocols mlp lookup culprit-flows
<get-ddos-mlp-lookup-flows>
show ddos-protection protocols mlp macpin-exception
<get-ddos-mlp-mac-pinning>
show ddos-protection protocols mlp macpin-exception culprit-flows
<get-ddos-mlp-mac-pinning-flows>
show ddos-protection protocols mlp aging-exception
<get-ddos-mlp-aging-exc>
show ddos-protection protocols mlp packets
<get-ddos-mlp-packets>
show ddos-protection protocols mlp parameters
<get-ddos-mlp-parameters>
show ddos-protection protocols mlp statistics
<get-ddos-mlp-statistics>
show ddos-protection protocols mlp unclassified
<get-ddos-mlp-unclass>
show ddos-protection protocols mlp violations
<get-ddos-mlp-violations>
show ddos-protection protocols msdp
<get-ddos-msdp-information>
show ddos-protection protocols msdp aggregate
<get-ddos-msdp-aggregate>
show ddos-protection protocols msdp parameters
<get-ddos-msdp-parameters>
show ddos-protection protocols msdp statistics
<get-ddos-msdp-statistics>
show ddos-protection protocols msdp violations
<get-ddos-msdp-violations>
show ddos-protection protocols msdpv6
<get-ddos-msdpv6-information>
show ddos-protection protocols msdpv6 aggregate
<get-ddos-msdpv6-aggregate>
show ddos-protection protocols msdpv6 parameters
<get-ddos-msdpv6-parameters>
show ddos-protection protocols msdpv6 statistics
<get-ddos-msdpv6-statistics>
show ddos-protection protocols msdpv6 violations
<get-ddos-msdpv6-violations>
show ddos-protection protocols multihop-bfd
<get-ddos-mhop-bfd-information>
show ddos-protection protocols multihop-bfd aggregate
<get-ddos-mhop-bfd-aggregate>
show ddos-protection protocols multihop-bfd aggregate culprit-flows
<get-ddos-mhop-bfd-aggregate-flows>
show ddos-protection protocols multihop-bfd culprit-flows
<get-ddos-mhop-bfd-flows>
show ddos-protection protocols multihop-bfd flow-detection
<get-ddos-mhop-bfd-flow-parameters>
show ddos-protection protocols multihop-bfd parameters
<get-ddos-mhop-bfd-parameters>
show ddos-protection protocols multihop-bfd statistics
<get-ddos-mhop-bfd-statistics>
show ddos-protection protocols multihop-bfd violations
<get-ddos-mhop-bfd-violations>
show ddos-protection protocols multicast-copy
<get-ddos-mcast-copy-information>
show ddos-protection protocols multicast-copy aggregate
<get-ddos-mcast-copy-aggregate>
show ddos-protection protocols multicast-copy parameters
<get-ddos-mcast-copy-parameters>
show ddos-protection protocols multicast-copy statistics
<get-ddos-mcast-copy-statistics>
show ddos-protection protocols multicast-copy violations
<get-ddos-mcast-copy-violations>
show ddos-protection protocols mvrp
<get-ddos-mvrp-information>
show ddos-protection protocols mvrp aggregate
<get-ddos-mvrp-aggregate>
show ddos-protection protocols mvrp parameters
<get-ddos-mvrp-parameters>
show ddos-protection protocols mvrp statistics
<get-ddos-mvrp-statistics>
show ddos-protection protocols mvrp violations
<get-ddos-mvrp-violations>
show ddos-protection protocols ndpv6
<get-ddos-ndpv6-information>
show ddos-protection protocols ndpv6 aggregate
<get-ddos-ndpv6-aggregate>
show ddos-protection protocols ndpv6 aggregate culprit-flows
<get-ddos-ndpv6-aggregate-flows>
show ddos-protection protocols ndpv6 culprit-flows
<get-ddos-ndpv6-flows>
show ddos-protection protocols ndpv6 flow-detection
<get-ddos-ndpv6-flow-parameters>
show ddos-protection protocols ndpv6 neighbor-advertisement
<get-ddos-ndpv6-neighbor-adv>
show ddos-protection protocols ndpv6 neighbor-advertisement culprit-flows
<get-ddos-ndpv6-neighb-adv-flows>
show ddos-protection protocols ndpv6 neighbor-solicitation
<get-ddos-ndpv6-neighb-sol>
show ddos-protection protocols ndpv6 neighbor-solicitation culprit-flows
<get-ddos-ndpv6-neighb-sol-flows>
show ddos-protection protocols ndpv6 parameters
<get-ddos-ndpv6-parameters>
show ddos-protection protocols ndpv6 redirect
<get-ddos-ndpv6-redirect>
show ddos-protection protocols ndpv6 redirect culprit-flows
<get-ddos-ndpv6-redirect-flows>
show ddos-protection protocols ndpv6 router-advertisement
<get-ddos-ndpv6-router-adv>
show ddos-protection protocols ndpv6 router-advertisement culprit-flows
<get-ddos-ndpv6-router-adv-flows>
show ddos-protection protocols ndpv6 router-solicitation
<get-ddos-ndpv6-router-sol>
show ddos-protection protocols ndpv6 router-solicitation culprit-flows
<get-ddos-ndpv6-router-sol-flows>
show ddos-protection protocols nonucast-switch
<get-ddos-nonucast-switch-information>
show ddos-protection protocols nonucast-switch aggregate
<get-ddos-nonucast-switch-aggregate>
show ddos-protection protocols nonucast-switch aggregate culprit-flows
<get-ddos-nonucast-switch-aggregate-flows>
show ddos-protection protocols nonucast-switch culprit-flows
<get-ddos-nonucast-switch-flows>
show ddos-protection protocols nonucast-switch flow-detection
<get-ddos-nonucast-switch-flow-parameters>
show ddos-protection protocols nonucast-switch parameters
<get-ddos-nonucast-switch-parameters>
show ddos-protection protocols nonucast-switch statistics
<get-ddos-nonucast-switch-statistics>
show ddos-protection protocols nonucast-switch violations
<get-ddos-nonucast-switch-violations>
show ddos-protection protocols ntp
get-ddos-ntp-information
show ddos-protection protocols ntp aggregate
get-ddos-ntp-aggregate
show ddos-protection protocols ntp parameters
get-ddos-ntp-parameters
show ddos-protection protocols ntp statistics
get-ddos-ntp-statistics
show ddos-protection protocols ntp violations
get-ddos-ntp-violations
show ddos-protection protocols oam-cfm
get-ddos-oam-cfm-information
show ddos-protection protocols oam-cfm aggregate
<get-ddos-oam-cfm-aggregate>
show ddos-protection protocols oam-cfm aggregate culprit-flows
<get-ddos-oam-cfm-aggregate-flows>
show ddos-protection protocols oam-cfm culprit-flows
<get-ddos-oam-cfm-flows>
show ddos-protection protocols oam-cfm flow-detection
<get-ddos-oam-cfm-flow-parameters>
show ddos-protection protocols oam-cfm parameters
<get-ddos-oam-cfm-parameters>
show ddos-protection protocols oam-cfm statistics
<get-ddos-oam-cfm-statistics>
show ddos-protection protocols oam-cfm violations
<get-ddos-oam-cfm-violations>
show ddos-protection protocols oam-lfm
get-ddos-oam-lfm-information
show ddos-protection protocols oam-lfm aggregate
get-ddos-oam-lfm-aggregate
show ddos-protection protocols oam-lfm parameters
get-ddos-oam-lfm-parameters
show ddos-protection protocols oam-lfm statistics
<get-ddos-oam-lfm-statistics>
show ddos-protection protocols oam-lfm violations
<get-ddos-oam-lfm-violations>
show ddos-protection protocols ospf
get-ddos-ospf-information
show ddos-protection protocols ospf aggregate
get-ddos-ospf-aggregate
show ddos-protection protocols ospf parameters
get-ddos-ospf-parameters
show ddos-protection protocols ospf statistics
<get-ddos-ospf-statistics>
show ddos-protection protocols ospf violations
<get-ddos-ospf-violations>
show ddos-protection protocols ospf-hello
<get-ddos-ospf-hello-information>
show ddos-protection protocols ospf-hello aggregate
<get-ddos-ospf-hello-aggregate>
show ddos-protection protocols ospf-hello aggregate culprit-flows
<get-ddos-ospf-hello-aggregate-flows>
show ddos-protection protocols ospf-hello culprit-flows
<get-ddos-ospf-hello-flows>
show ddos-protection protocols ospf-hello flow-detection
<get-ddos-ospf-hello-flow-parameters>
show ddos-protection protocols ospf-hello parameters
<get-ddos-ospf-hello-parameters>
show ddos-protection protocols ospf-hello statistics
<get-ddos-ospf-hello-statistics>
show ddos-protection protocols ospf-hello violations
<get-ddos-ospf-hello-violations>
show ddos-protection protocols ospfv3v6
  get-ddos-ospfv3v6-information
show ddos-protection protocols ospfv3v6 aggregate
  get-ddos-ospfv3v6-aggregate
show ddos-protection protocols ospfv3v6 parameters
  get-ddos-ospfv3v6-parameters
show ddos-protection protocols ospfv3v6 statistics
  get-ddos-ospfv3v6-statistics
show ddos-protection protocols ospfv3v6 violations
  get-ddos-ospfv3v6-violations
show ddos-protection protocols parameters
  get-ddos-protocols-parameters
show ddos-protection protocols pfe-alive
  get-ddos-pfe-alive-information
show ddos-protection protocols pfe-alive aggregate
  get-ddos-pfe-alive-aggregate
show ddos-protection protocols pfe-alive parameters
  get-ddos-pfe-alive-parameters
show ddos-protection protocols pfe-alive statistics
  get-ddos-pfe-alive-statistics
show ddos-protection protocols pfe-alive violations
  get-ddos-pfe-alive-violations
show ddos-protection protocols pim
  get-ddos-pim-information
show ddos-protection protocols pim aggregate
  get-ddos-pim-aggregate
show ddos-protection protocols pim aggregate culprit-flows
show ddos-protection protocols pim parameters
  get-ddos-pim-parameters
show ddos-protection protocols pim statistics
  get-ddos-pim-statistics
show ddos-protection protocols pim violations
  get-ddos-pim-violations
show ddos-protection protocols pim-ctrl
  <get-ddos-pim-ctrl-information>
show ddos-protection protocols pim-ctrl aggregate
  <get-ddos-pim-ctrl-aggregate>
show ddos-protection protocols pim-ctrl aggregate culprit-flows
  <get-ddos-pim-ctrl-aggregate-flows>
show ddos-protection protocols pim-ctrl culprit-flows
  <get-ddos-pim-ctrl-flows>
show ddos-protection protocols pim-ctrl flow-detection
  <get-ddos-pim-ctrl-flow-parameters>
show ddos-protection protocols pim-ctrl parameters
  <get-ddos-pim-ctrl-parameters>
show ddos-protection protocols pim-ctrl statistics
  <get-ddos-pim-ctrl-statistics>
show ddos-protection protocols pim-ctrl violations
  <get-ddos-pim-ctrl-violations>
show ddos-protection protocols pim-data
  <get-ddos-pim-data-information>
show ddos-protection protocols pim-data aggregate
  <get-ddos-pim-data-aggregate>
show ddos-protection protocols pim-data aggregate culprit-flows
  <get-ddos-pim-data-aggregate-flows>
show ddos-protection protocols pim-data culprit-flows
  <get-ddos-pim-data-flows>
show ddos-protection protocols pim-data flow-detection
  <get-ddos-pim-data-flow-parameters>
show ddos-protection protocols pim-data parameters
  <get-ddos-pim-data-parameters>
show ddos-protection protocols pim-data statistics
  <get-ddos-pim-data-statistics>
show ddos-protection protocols pim-data violations
  <get-ddos-pim-data-violations>
show ddos-protection protocols pimv6
  <get-ddos-pimv6-information>
show ddos-protection protocols pimv6 aggregate
  <get-ddos-pimv6-aggregate>
show ddos-protection protocols pimv6 aggregate culprit-flows
show ddos-protection protocols pimv6 parameters
<get-ddos-pimv6-parameters>
show ddos-protection protocols pimv6 statistics
<get-ddos-pimv6-statistics>
show ddos-protection protocols pimv6 violations
<get-ddos-pimv6-violations>
show ddos-protection protocols pkt-inject
<get-ddos-pkt-inject-information>
show ddos-protection protocols pkt-inject aggregate
<get-ddos-pkt-inject-aggregate>
show ddos-protection protocols pkt-inject aggregate culprit-flows
<get-ddos-pkt-inject-aggregate-flows>
show ddos-protection protocols pkt-inject culprit-flows
<get-ddos-pkt-inject-flows>
show ddos-protection protocols pkt-inject flow-detection
<get-ddos-pkt-inject-flow-parameters>
show ddos-protection protocols pkt-inject parameters
<get-ddos-pkt-inject-parameters>
show ddos-protection protocols pkt-inject statistics
<get-ddos-pkt-inject-statistics>
show ddos-protection protocols pkt-inject violations
<get-ddos-pkt-inject-violations>

show ddos-protection protocols pmvrp
  get-ddos-pmvrp-information
show ddos-protection protocols pmvrp aggregate
  get-ddos-pmvrp-aggregate
show ddos-protection protocols pmvrp parameters
  get-ddos-pmvrp-parameters
show ddos-protection protocols pmvrp statistics
  get-ddos-pmvrp-statistics
show ddos-protection protocols pmvrp violations
  get-ddos-pmvrp-violations
show ddos-protection protocols pos
  get-ddos-pos-information
show ddos-protection protocols pos aggregate
  get-ddos-pos-aggregate
show ddos-protection protocols pos aggregate culprit-flows
show ddos-protection protocols pos parameters
  get-ddos-pos-parameters
show ddos-protection protocols pos statistics
  get-ddos-pos-statistics
show ddos-protection protocols pos violations
  get-ddos-pos-violations
show ddos-protection protocols ppp
  get-ddos-ppp-information
show ddos-protection protocols ppp aggregate
  get-ddos-ppp-aggregate
show ddos-protection protocols ppp authentication
  get-ddos-ppp-auth
show ddos-protection protocols ppp authentication culprit-flows
show ddos-protection protocols ppp ipcp
  get-ddos-ppp-ipcp
show ddos-protection protocols ppp ipv6cp
  get-ddos-ppp-ipv6cp
show ddos-protection protocols ppp isis
  get-ddos-ppp-isis
show ddos-protection protocols ppp isis culprit-flows
show ddos-protection protocols ppp lcp
  get-ddos-ppp-lcp
show ddos-protection protocols ppp lcp culprit-flows
show ddos-protection protocols ppp mplscp
  get-ddos-ppp-mplscp
show ddos-protection protocols ppp mplscp culprit-flows
show ddos-protection protocols ppp parameters
  get-ddos-ppp-parameters
show ddos-protection protocols ppp statistics
  get-ddos-ppp-statistics
show ddos-protection protocols ppp unclassified
  <get-ddos-ppp-unclass>
show ddos-protection protocols ppp violations
  get-ddos-ppp-violations
show ddos-protection protocols pppoe
  get-ddos-pppoe-information
show ddos-protection protocols pppoe aggregate
  get-ddos-pppoe-aggregate
show ddos-protection protocols pppoe padi
  get-ddos-pppoe-padi
show ddos-protection protocols pppoe padm
  get-ddos-pppoe-padm
show ddos-protection protocols pppoe padn
  get-ddos-pppoe-padn
show ddos-protection protocols pppoe pado
  get-ddos-pppoe-pado
show ddos-protection protocols pppoe padr
  get-ddos-pppoe-padr
show ddos-protection protocols pppoe pads
  get-ddos-pppoe-pads
show ddos-protection protocols pppoe padt
  get-ddos-pppoe-padt
show ddos-protection protocols pppoe parameters
  get-ddos-pppoe-parameters
show ddos-protection protocols pppoe statistics
  get-ddos-pppoe-statistics
show ddos-protection protocols pppoe violations
  get-ddos-pppoe-violations
show ddos-protection protocols proto-802-1x
<get-ddos-8021x-information>
show ddos-protection protocols proto-802-1x aggregate
<get-ddos-8021x-aggregate>
show ddos-protection protocols proto-802-1x aggregate culprit-flows
  get-ddos-8021x-aggregate-flows
show ddos-protection protocols proto-802-1x culprit-flows
  <get-ddos-8021x-flows>
show ddos-protection protocols proto-802-1x flow-detection
  <get-ddos-8021x-flow-parameters>
show ddos-protection protocols proto-802-1x parameters
  <get-ddos-8021x-parameters>
show ddos-protection protocols proto-802-1x statistics
  <get-ddos-8021x-statistics>
show ddos-protection protocols proto-802-1x violations
  <get-ddos-8021x-violations>
show ddos-protection protocols ptp
  get-ddos-ptp-information
show ddos-protection protocols ptp aggregate
  get-ddos-ptp-aggregate
show ddos-protection protocols ptp aggregate culprit-flows
show ddos-protection protocols ptp parameters
  get-ddos-ptp-parameters
show ddos-protection protocols ptp statistics
  get-ddos-ptp-statistics
show ddos-protection protocols ptp violations
  get-ddos-ptp-violations
show ddos-protection protocols ptpv6
<get-ddos-ptpv6-information>
show ddos-protection protocols ptpv6 aggregate
<get-ddos-ptpv6-aggregate>
show ddos-protection protocols ptpv6 aggregate culprit-flows
<get-ddos-ptpv6-aggregate-flows>
show ddos-protection protocols ptpv6 culprit-flows
<get-ddos-ptpv6-flows>
show ddos-protection protocols ptpv6 flow-detection
<get-ddos-ptpv6-flow-parameters>
show ddos-protection protocols ptpv6 parameters
<get-ddos-ptpv6-parameters>
show ddos-protection protocols ptpv6 statistics
<get-ddos-ptpv6-statistics>
show ddos-protection protocols ptpv6 violations
<get-ddos-ptpv6-violations>
show ddos-protection protocols pvstp
  get-ddos-pvstp-information
show ddos-protection protocols pvstp aggregate
  get-ddos-pvstp-aggregate
show ddos-protection protocols pvstp parameters
  get-ddos-pvstp-parameters
show ddos-protection protocols pvstp statistics
  get-ddos-pvstp-statistics
show ddos-protection protocols pvstp violations
  get-ddos-pvstp-violations
show ddos-protection protocols radius
  get-ddos-radius-information
show ddos-protection protocols radius accounting
  get-ddos-radius-account
show ddos-protection protocols radius aggregate
  get-ddos-radius-aggregate
show ddos-protection protocols radius accounting culprit-flows
show ddos-protection protocols radius authorization
  get-ddos-radius-auth
show ddos-protection protocols radius parameters
  get-ddos-radius-parameters
show ddos-protection protocols radius server
  get-ddos-radius-server
show ddos-protection protocols radius statistics
  get-ddos-radius-statistics
show ddos-protection protocols radius violations
  get-ddos-radius-violations
show ddos-protection protocols re-services
<get-ddos-re-services-information>
show ddos-protection protocols re-services aggregate
  <get-ddos-re-services-aggregate>
show ddos-protection protocols re-services aggregate culprit-flows
  <get-ddos-re-services-aggregate-flows>
show ddos-protection protocols re-services captive-portal
  <get-ddos-re-services-captive-portal>
show ddos-protection protocols re-services captive-portal culprit-flows
  <get-ddos-re-services-captive-portal-flows>
show ddos-protection protocols re-services culprit-flows
  <get-ddos-re-services-flows>
show ddos-protection protocols re-services flow-detection
  <get-ddos-re-services-flow-parameters>
show ddos-protection protocols re-services parameters
  <get-ddos-re-services-parameters>
show ddos-protection protocols re-services statistics
  <get-ddos-re-services-statistics>
show ddos-protection protocols re-services violations
  <get-ddos-re-services-violations>
show ddos-protection protocols re-services-v6
  <get-ddos-re-services-v6-information>
show ddos-protection protocols re-services-v6 aggregate
  <get-ddos-re-services-v6-aggregate>
show ddos-protection protocols re-services-v6 aggregate culprit-flows
  <get-ddos-re-services-v6-aggregate-flows>
show ddos-protection protocols re-services-v6 captive-portal
  <get-ddos-re-services-v6-captive-portal-v6>
show ddos-protection protocols re-services-v6 captive-portal culprit-flows
  <get-ddos-re-services-v6-captive-portal-v6-flows>
show ddos-protection protocols re-services-v6 culprit-flows
  <get-ddos-re-services-v6-flows>
show ddos-protection protocols re-services-v6 flow-detection
  <get-ddos-re-services-v6-flow-parameters>
show ddos-protection protocols re-services-v6 parameters
  <get-ddos-re-services-v6-parameters>
show ddos-protection protocols re-services-v6 statistics
  <get-ddos-re-services-v6-statistics>
show ddos-protection protocols re-services-v6 violations
  <get-ddos-re-services-v6-violations>
show ddos-protection protocols redirect
  get-ddos-redirect-information
show ddos-protection protocols redirect aggregate
  get-ddos-redirect-aggregate
show ddos-protection protocols redirect parameters
  get-ddos-redirect-parameters
show ddos-protection protocols redirect statistics
  get-ddos-redirect-statistics
show ddos-protection protocols redirect violations
  get-ddos-redirect-violations

show ddos-protection protocols reject
  <get-ddos-reject-information>
show ddos-protection protocols reject aggregate
  <get-ddos-reject-aggregate>
show ddos-protection protocols reject parameters
  <get-ddos-reject-parameters>
show ddos-protection protocols reject statistics
  <get-ddos-reject-statistics>
show ddos-protection protocols reject violations
  <get-ddos-reject-violations>
show ddos-protection protocols rejectv6
  show ddos-protection protocols rejectv6 aggregate
  show ddos-protection protocols rejectv6 aggregate culprit-flows
  show ddos-protection protocols rejectv6 flow-detection
  show ddos-protection protocols rejectv6 parameters
  show ddos-protection protocols rejectv6 statistics
  show ddos-protection protocols rejectv6 violations
show ddos-protection protocols rip
  get-ddos-rip-information
show ddos-protection protocols rip aggregate
  get-ddos-rip-aggregate
show ddos-protection protocols rip aggregate culprit-flows
show ddos-protection protocols rip culprit-flows
show ddos-protection protocols rip parameters
  get-ddos-rip-parameters
show ddos-protection protocols rip statistics
  get-ddos-rip-statistics
show ddos-protection protocols rip violations
  get-ddos-rip-violations
show ddos-protection protocols ripv6
  get-ddos-ripv6-information
show ddos-protection protocols ripv6 aggregate
  get-ddos-ripv6-aggregate
show ddos-protection protocols ripv6 aggregate culprit-flows
show ddos-protection protocols ripv6 parameters
get-ddos-ripv6-parameters
show ddos-protection protocols ripv6 statistics
get-ddos-ripv6-statistics
show ddos-protection protocols ripv6 violations
get-ddos-ripv6-violations
show ddos-protection protocols rsvp
get-ddos-rsvp-information
show ddos-protection protocols rsvp aggregate
get-ddos-rsvp-aggregate
show ddos-protection protocols rsvp aggregate culprit-flows
get-ddos-rsvp-aggregate
show ddos-protection protocols rsvp parameters
get-ddos-rsvp-parameters
show ddos-protection protocols rsvp statistics
get-ddos-rsvp-statistics
show ddos-protection protocols rsvp violations
get-ddos-rsvp-violations
show ddos-protection protocols rsvpv6
get-ddos-rsvpv6-information
show ddos-protection protocols rsvpv6 aggregate
get-ddos-rsvpv6-aggregate
show ddos-protection protocols rsvpv6 aggregate culprit-flows
get-ddos-rsvpv6-aggregate
show ddos-protection protocols rsvpv6 parameters
get-ddos-rsvpv6-parameters
show ddos-protection protocols rsvpv6 statistics
get-ddos-rsvpv6-statistics
show ddos-protection protocols rsvpv6 violations
get-ddos-rsvpv6-violations
show ddos-protection protocols sample
<get-ddos-sample-information>
show ddos-protection protocols sample aggregate
<get-ddos-sample-aggregate>
show ddos-protection protocols sample aggregate culprit-flows
<get-ddos-sample-host>
show ddos-protection protocols sample parameters
<get-ddos-sample-parameters>
show ddos-protection protocols sample pfe
<get-ddos-sample-pfe>
show ddos-protection protocols sample pfe culprit-flows
<get-ddos-sample-sflow>
show ddos-protection protocols sample sflow culprit-flows
<get-ddos-sample-sflow-flows>
show ddos-protection protocols sample statistics
<get-ddos-sample-statistics>
show ddos-protection protocols sample syslog
show ddos-protection protocols sample tap
<get-ddos-sample-tap>
show ddos-protection protocols sample tap culprit-flows
show ddos-protection protocols sample violations
<get-ddos-sample-violations>
show ddos-protection protocols services
    get-ddos-services-information
show ddos-protection protocols sample-dest
<get-ddos-sample-dest-information>
show ddos-protection protocols sample-dest aggregate
<get-ddos-sample-dest-aggregate>
show ddos-protection protocols sample-dest aggregate culprit-flows
<get-ddos-sample-dest-aggregate-flows>
show ddos-protection protocols sample-dest culprit-flows
<get-ddos-sample-dest-flows>
show ddos-protection protocols sample-dest flow-detection
<get-ddos-sample-dest-flow-parameters>
show ddos-protection protocols sample-dest parameters
<get-ddos-sample-dest-parameters>
show ddos-protection protocols sample-dest statistics
<get-ddos-sample-dest-statistics>
show ddos-protection protocols sample-dest violations
<get-ddos-sample-dest-violations>
show ddos-protection protocols sample-source
<get-ddos-sample-source-information>
show ddos-protection protocols sample-source aggregate
<get-ddos-sample-source-aggregate>
show ddos-protection protocols sample-source aggregate culprit-flows
<get-ddos-sample-source-aggregate-flows>
show ddos-protection protocols sample-source aggregate culprit-flows
<get-ddos-sample-source-aggregate-flows>
show ddos-protection protocols sample-source culprit-flows
<get-ddos-sample-source-flows>
show ddos-protection protocols sample-source flow-detection
<get-ddos-sample-source-flow-parameters>
show ddos-protection protocols sample-source parameters
<get-ddos-sample-source-parameters>
show ddos-protection protocols sample-source statistics
<get-ddos-sample-source-statistics>
show ddos-protection protocols sample-source violations
  <get-ddos-sample-source-violations>
show ddos-protection protocols services aggregate
  <get-ddos-services-aggregate>
show ddos-protection protocols services parameters
  <get-ddos-services-parameters>
show ddos-protection protocols services statistics
  <get-ddos-services-statistics>
show ddos-protection protocols syslog
  <get-ddos-syslog-information>
show ddos-protection protocols syslog aggregate
  <get-ddos-syslog-aggregate>
show ddos-protection protocols syslog aggregate culprit-flows
  <get-ddos-syslog-aggregate-flows>
show ddos-protection protocols syslog culprit-flows
  <get-ddos-syslog-flows>
show ddos-protection protocols syslog flow-detection
  <get-ddos-syslog-flow-parameters>
show ddos-protection protocols syslog parameters
  <get-ddos-syslog-parameters>
show ddos-protection protocols syslog statistics
  <get-ddos-syslog-statistics>
show ddos-protection protocols syslog violations
  <get-ddos-syslog-violations>
show ddos-protection protocols services violations
  get-ddos-services-violations
show ddos-protection protocols snmp
  get-ddos-snmp-information
show ddos-protection protocols snmp aggregate
  get-ddos-snmp-aggregate
show ddos-protection protocols snmp aggregate culprit-flows
show ddos-protection protocols snmp parameters
  get-ddos-snmp-parameters
show ddos-protection protocols snmp statistics
  get-ddos-snmp-statistics
show ddos-protection protocols snmp violations
  get-ddos-snmp-violations
show ddos-protection protocols snmpv6
  get-ddos-snmpv6-information
show ddos-protection protocols snmpv6 aggregate
  get-ddos-snmpv6-aggregate
show ddos-protection protocols snmpv6 aggregate culprit-flows
show ddos-protection protocols snmpv6 parameters
  get-ddos-snmpv6-parameters
show ddos-protection protocols snmpv6 statistics
  get-ddos-snmpv6-statistics
show ddos-protection protocols snmpv6 violations
  get-ddos-snmpv6-violations
show ddos-protection protocols ssh
  get-ddos-ssh-information
show ddos-protection protocols ssh aggregate
  get-ddos-ssh-aggregate
show ddos-protection protocols ssh parameters
  get-ddos-ssh-parameters
show ddos-protection protocols ssh statistics
  get-ddos-ssh-statistics
show ddos-protection protocols ssh violations
  get-ddos-ssh-violations
show ddos-protection protocols sshv6
  get-ddos-sshv6-information
show ddos-protection protocols sshv6 aggregate
  get-ddos-sshv6-aggregate
show ddos-protection protocols sshv6 parameters
  get-ddos-sshv6-parameters
show ddos-protection protocols sshv6 statistics
  get-ddos-sshv6-statistics
show ddos-protection protocols sshv6 violations
  get-ddos-sshv6-violations
show ddos-protection protocols statistics
  get-ddos-protocols-statistics
show ddos-protection protocols stp
  get-ddos-stp-information
show ddos-protection protocols stp aggregate
  get-ddos-stp-aggregate
show ddos-protection protocols stp parameters
  get-ddos-stp-parameters
show ddos-protection protocols stp statistics
  get-ddos-stp-statistics
show ddos-protection protocols stp violations
  get-ddos-stp-violations
show ddos-protection protocols tacacs
  get-ddos-tacacs-information
show ddos-protection protocols tacacs aggregate
  get-ddos-tacacs-aggregate
show ddos-protection protocols tacacs parameters
  <get-ddos-tacacs-parameters>
show ddos-protection protocols tacacs statistics
  <get-ddos-tacacs-statistics>
show ddos-protection protocols tacacs violations
  <get-ddos-tacacs-violations>

show ddos-protection protocols tcc
  <get-ddos-tcc-information>
show ddos-protection protocols tcc aggregate
  <get-ddos-tcc-aggregate>
show ddos-protection protocols tcc aggregate culprit-flows
  <get-ddos-tcc-aggregate-flows>
show ddos-protection protocols tcc culprit-flows
  <get-ddos-tcc-flows>
show ddos-protection protocols tcc ethernet-tcc
  <get-ddos-tcc-ethernet-tcc>
show ddos-protection protocols tcc ethernet-tcc culprit-flows
  <get-ddos-tcc-ethernet-tcc-flows>
show ddos-protection protocols tcc flow-detection
  <get-ddos-tcc-flow-parameters>
show ddos-protection protocols tcc iso-tcc
  <get-ddos-tcc-iso-tcc>
show ddos-protection protocols tcc iso-tcc culprit-flows
  <get-ddos-tcc-iso-tcc-flows>
show ddos-protection protocols tcc parameters
  <get-ddos-tcc-parameters>
show ddos-protection protocols tcc statistics
  <get-ddos-tcc-statistics>
show ddos-protection protocols tcc unclassified
  <get-ddos-tcc-unclass>
show ddos-protection protocols tcc unclassified culprit-flows
  <get-ddos-tcc-unclass-flows>
show ddos-protection protocols tcc violations
  <get-ddos-tcc-violations>
show ddos-protection protocols tcp-flags
  <get-ddos-tcp-flags-information>
show ddos-protection protocols tcp-flags aggregate
  <get-ddos-tcp-flags-aggregate>
show ddos-protection protocols tcp-flags established
  <get-ddos-tcp-flags-establish>
show ddos-protection protocols tcp-flags initial
<get-ddos-tcp-flags-initial>
show ddos-protection protocols tcp-flags parameters
<get-ddos-tcp-flags-parameters>
show ddos-protection protocols tcp-flags statistics
<get-ddos-tcp-flags-statistics>
show ddos-protection protocols tcp-flags unclassified
<get-ddos-tcp-flags-unclass>
show ddos-protection protocols tcp-flags violations
<get-ddos-tcp-flags-violations>
show ddos-protection protocols telnet
<get-ddos-telnet-information>
show ddos-protection protocols telnet aggregate
<get-ddos-telnet-aggregate>
show ddos-protection protocols telnet aggregate culprit-flows
show ddos-protection protocols telnet parameters
<get-ddos-telnet-parameters>
show ddos-protection protocols telnet statistics
<get-ddos-telnet-statistics>
show ddos-protection protocols telnet violations
<get-ddos-telnet-violations>
show ddos-protection protocols telnetv6
<get-ddos-telnetv6-information>
show ddos-protection protocols telnetv6 aggregate
<get-ddos-telnetv6-aggregate>
show ddos-protection protocols telnetv6 aggregate culprit-flows
show ddos-protection protocols telnetv6 parameters
<get-ddos-telnetv6-parameters>
show ddos-protection protocols telnetv6 statistics
<get-ddos-telnetv6-statistics>
show ddos-protection protocols telnetv6 violations
<get-ddos-telnetv6-violations>
show ddos-protection protocols ttl
<get-ddos-ttl-information>
show ddos-protection protocols ttl aggregate
<get-ddos-ttl-aggregate>
show ddos-protection protocols ttl parameters
<get-ddos-ttl-parameters>
show ddos-protection protocols ttl statistics
<get-ddos-ttl-statistics>
show ddos-protection protocols ttl violations
<get-ddos-ttl-violations>
show ddos-protection protocols tunnel-fragment
<get-ddos-tun-frag-information>
show ddos-protection protocols tunnel-fragment aggregate
<get-ddos-tun-frag-aggregate>
show ddos-protection protocols tunnel-fragment aggregate culprit-flows
show ddos-protection protocols tunnel-fragment parameters
<get-ddos-tun-frag-parameters>
show ddos-protection protocols tunnel-fragment statistics
<get-ddos-tun-frag-statistics>
show ddos-protection protocols tunnel-fragment violations
<get-ddos-tun-frag-violations>
show ddos-protection protocols tunnel-ka
<get-ddos-tunnel-ka-information>
show ddos-protection protocols tunnel-ka aggregate
<get-ddos-tunnel-ka-aggregate>
show ddos-protection protocols tunnel-ka aggregate culprit-flows
<get-ddos-tunnel-ka-aggregate-flows>
show ddos-protection protocols tunnel-ka culprit-flows
<get-ddos-tunnel-ka-flows>
show ddos-protection protocols tunnel-ka flow-detection
<get-ddos-tunnel-ka-flow-parameters>
show ddos-protection protocols tunnel-ka parameters
<get-ddos-tunnel-ka-parameters>
show ddos-protection protocols tunnel-ka statistics
<get-ddos-tunnel-ka-statistics>
show ddos-protection protocols tunnel-ka violations
<get-ddos-tunnel-ka-violations>
show ddos-protection protocols unknown-12mc
<get-ddos-unknown-12mc-information>
show ddos-protection protocols unknown-12mc aggregate
<get-ddos-unknown-12mc-aggregate>
show ddos-protection protocols unknown-12mc aggregate culprit-flows
<get-ddos-unknown-12mc-aggregate-flows>
show ddos-protection protocols unknown-12mc culprit-flows
<get-ddos-unknown-12mc-flows>
show ddos-protection protocols unknown-12mc flow-detection
<get-ddos-unknown-12mc-flow-parameters>
show ddos-protection protocols unknown-12mc parameters
<get-ddos-unknown-12mc-parameters>
show ddos-protection protocols unknown-12mc statistics
<get-ddos-unknown-12mc-statistics>
show ddos-protection protocols unknown-12mc violations
<get-ddos-unknown-12mc-violations>
show ddos-protection protocols unclassified
  <get-ddos-uncls-information>
show ddos-protection protocols unclassified aggregate
  <get-ddos-uncls-aggregate>
show ddos-protection protocols unclassified parameters
  <get-ddos-uncls-parameters>
show ddos-protection protocols unclassified resolve-v4
show ddos-protection protocols unclassified resolve-v4 culprit-flows
show ddos-protection protocols unclassified resolve-v6
show ddos-protection protocols unclassified resolve-v6 culprit-flows
show ddos-protection protocols unclassified statistics
  <get-ddos-uncls-statistics>
show ddos-protection protocols unclassified violations
  <get-ddos-uncls-violations>
show ddos-protection protocols urpf-fail
  <get-ddos-urpf-fail-information>
show ddos-protection protocols urpf-fail aggregate
  <get-ddos-urpf-fail-aggregate>
show ddos-protection protocols urpf-fail aggregate culprit-flows
  <get-ddos-urpf-fail-aggregate-flows>
show ddos-protection protocols urpf-fail culprit-flows
  <get-ddos-urpf-fail-flows>
show ddos-protection protocols urpf-fail flow-detection
  <get-ddos-urpf-fail-flow-parameters>
show ddos-protection protocols urpf-fail parameters
  <get-ddos-urpf-fail-parameters>
show ddos-protection protocols urpf-fail statistics
  <get-ddos-urpf-fail-statistics>
show ddos-protection protocols urpf-fail violations
  <get-ddos-urpf-fail-violations>
show ddos-protection protocols vcipc-udp
  <get-ddos-vcipc-udp-information>
show ddos-protection protocols vcipc-udp aggregate
  <get-ddos-vcipc-udp-aggregate>
show ddos-protection protocols vcipc-udp aggregate culprit-flows
  <get-ddos-vcipc-udp-aggregate-flows>
show ddos-protection protocols vcipc-udp culprit-flows
  <get-ddos-vcipc-udp-flows>
show ddos-protection protocols vcipc-udp flow-detection
  <get-ddos-vcipc-udp-flow-parameters>
show ddos-protection protocols vcipc-udp parameters
  <get-ddos-vcipc-udp-parameters>
show ddos-protection protocols vcipc-udp statistics
  <get-ddos-vcipc-udp-statistics>
show ddos-protection protocols vcipc-udp violations
  <get-ddos-vcipc-udp-violations>
show ddos-protection protocols violations
  get-ddos-protocols-violations
show ddos-protection protocols virtual-chassis
  get-ddos-vchassis-information
show ddos-protection protocols virtual-chassis aggregate
  get-ddos-vchassis-aggregate
show ddos-protection protocols virtual-chassis aggregate culprit-flows
show ddos-protection protocols virtual-chassis control-high
  get-ddos-vchassis-control-hi
show ddos-protection protocols virtual-chassis control-low
  get-ddos-vchassis-control-lo
show ddos-protection protocols virtual-chassis parameters
  get-ddos-vchassis-parameters
show ddos-protection protocols virtual-chassis statistics
  get-ddos-vchassis-statistics
show ddos-protection protocols virtual-chassis unclassified
  get-ddos-vchassis-unclass
show ddos-protection protocols virtual-chassis vc-packets
  get-ddos-vchassis-vc-packets
show ddos-protection protocols virtual-chassis vc-ttl-errors
  get-ddos-vchassis-vc-ttl-err
show ddos-protection protocols virtual-chassis violations
  get-ddos-vchassis-violations
show ddos-protection protocols vrrp
  get-ddos-vrrp-information
show ddos-protection protocols vrrp aggregate
  get-ddos-vrrp-aggregate
show ddos-protection protocols vrrp aggregate culprit-flows
show ddos-protection protocols vrrp parameters
  get-ddos-vrrp-parameters
show ddos-protection protocols vrrp statistics
  get-ddos-vrrp-statistics
show ddos-protection protocols vrrp violations
  get-ddos-vrrp-violations
show ddos-protection protocols vrrpv6
  get-ddos-vrrpv6-information
show ddos-protection protocols vrrpv6 aggregate
  get-ddos-vrrpv6-aggregate
show ddos-protection protocols vrrpv6 aggregate culprit-flows
show ddos-protection protocols vrrpv6 parameters
get-ddos-vrrpv6-parameters
show ddos-protection protocols vrrpv6 statistics
get-ddos-vrrpv6-statistics
show ddos-protection protocols vrrpv6 violations
get-ddos-vrrpv6-violations
show ddos-protection statistics
get-ddos-statistics-information
show ddos-protection version
get-ddos-version
show ddos-protection protocols vxlan
<get-ddos-vxlan-information>
show ddos-protection protocols vxlan aggregate
<get-ddos-vxlan-aggregate>
show ddos-protection protocols vxlan aggregate culprit-flows
<get-ddos-vxlan-aggregate-flows>
show ddos-protection protocols vxlan culprit-flows
<get-ddos-vxlan-flows>
show ddos-protection protocols vxlan flow-detection
<get-ddos-vxlan-flow-parameters>
show ddos-protection protocols vxlan parameters
<get-ddos-vxlan-parameters>
show ddos-protection protocols vxlan statistics
<get-ddos-vxlan-statistics>
show ddos-protection protocols vxlan violations
<get-ddos-vxlan-violations>
show dhcp
show dhcp proxy-client
show dhcp proxy-client binding
show dhcp proxy-client servers
show dhcp proxy-client statistics
<get-proxy-dhcp-client-statistics-information>
show dhcp relay
show dhcp relay binding
<get-dhcp-relay-binding-information>
show dhcp relay binding interface
<get-dhcp-relay-interface-bindings>
show dhcp relay binding lease-time-violation
<get-dhcp-relay-binding-ltv-information>
show dhcp relay statistics
<get-dhcp-relay-statistics-information>
show dhcp relay statistics bulk-leasequery-connections
<get-dhcp-relay-bulk-leasequery-conn-statistics>
show dhcp relay statistics leasequery
<get-dhcp-relay-leasequery-statistics>

show dhcp server
show dhcp server binding
<get-dhcp-server-binding-information>

show dhcp server binding interface
<get-dhcp-relay-binding-interface>
show dhcp server binding lease-time-violation
<get-dhcp-server-binding-ltv-information>
show dhcp server statistics
<get-dhcp-server-statistics-information>
show dhcp statistics
<get-dhcp-service-statistics-information>
show dhcp-security
<get-dhcp-security-arp-inspection-statistics>
show dhcp-security binding
<get-dhcp-security-binding>
show dhcp-security binding interface
<get-dhcp-security-binding-interface>
show dhcp-security binding ip-address
<get-dhcp-security-binding-ip-address>
show dhcp-security binding ip-source-guard
<get-dhcp-security-ip-source-guard>
show dhcp-security binding statistics
<get-dhcp-security-binding-statistics>
show dhcp-security binding vlan
<get-dhcp-security-binding-vlan>
show dhcp-security ipv6
show dhcp-security ipv6 binding
<get-dhcpv6-security-binding>
show dhcp-security ipv6 binding interface
<get-dhcpv6-security-binding-interface>
show dhcp-security ipv6 binding ipv6-address
<get-dhcpv6-security-binding-ipv6-address>
show dhcp-security ipv6 binding vlan
<get-dhcpv6-security-binding-vlan>
show dhcp-security ipv6 statistics
<get-dhcp-ipv6-statistics>
show dhcp-security neighbor-discovery-inspection
show dhcp-security neighbor-discovery-inspection statistics
<get-dhcp-security-nd-inspection-statistics>
show dhcp-security neighbor-discovery-inspection statistics interface
<get-dhcp-security-ndi-interface>
show dhcp-security statistics
<get-dhcp-security-statistics>

show dhcpv6
show dhcpv6 client
get-dhcpv6-client-binding-information
show dhcpv6 client binding interface
<get-dhcpv6-client-binding-information-by-interface>
show dhcpv6 client statistics
<get-dhcpv6-client-statistics-information>
show dhcpv6 proxy-client
show dhcpv6 proxy-client binding
show dhcpv6 proxy-client statistics
<get-proxy-dhcpv6-client-statistics-information>
show dhcpv6 relay
show dhcpv6 relay binding
<get-dhcpv6-relay-binding-information>
show dhcpv6 relay binding interface
<get-dhcpv6-relay-binding-interface>
show dhcpv6 relay binding lease-time-violation
<get-dhcpv6-relay-binding-ltv-information>
show dhcpv6 relay statistics
<get-dhcpv6-relay-statistics-information>
show dhcpv6 relay statistics bulk-leasequery-connections
<get-dhcpv6-relay-bulk-leasequery-conn-statistics>
show dhcpv6 relay statistics leasequery
<get-dhcpv6-relay-leasequery-statistics>
show dhcpv6 server
show dhcpv6 server binding
<get-dhcpv6-server-binding-information>

show dhcpv6 server binding interface
<get-dhcpv6-server-binding-interface>
show dhcpv6 server binding lease-time-violation
<get-dhcpv6-server-binding-ltv-information>
show dhcpv6 server statistics
   <get-dhcpv6-server-statistics-information>
show dhcpv6 server statistics bulk-leasequery-connections
   <get-dhcpv6-server-bulk-leasequery-conn-statistics>
show dhcpv6 statistics
   <get-dhcpv6-service-statistics-information>
show diagnostics
show diagnostics tdr
   <get-tdr-interface-information>
show diagnostics tdr interface
   <get-tdr-interface-status>
show diameter
   <get-diameter-information>
show diameter function
   <get-diameter-function-information>
show diameter function statistics
   <get-diameter-function-statistics>
show diameter instance
   <get-diameter-instance-information>
show diameter network-element
   <get-diameter-network-element-information>
show diameter network-element map
   <get-diameter-network-element-map-information>
show diameter peer
   <get-diameter-peer-information>
show diameter peer map
   <get-diameter-peer-map-information>
show diameter peer statistics
   <get-diameter-peer-statistics>
show diameter route
   <get-diameter-route-information>
show dot1x
show dot1x accounting-attributes
get-dot1x-accounting-attributes
show dot1x accounting-attributes interface
   <get-dot1x-interface-accounting-attributes>
show dot1x authentication-failed-users
   <get-dot1x-authentication-failed-users>
show dot1x interface
   <get-dot1x-interface-information>
show dot1x static-mac-address
   <get-dot1x-static-mac-addresses>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x static-mac-address interface</td>
<td>Get dot1x interface static-mac-address information</td>
</tr>
<tr>
<td>show dvmrp</td>
<td>Display DVMRP information</td>
</tr>
<tr>
<td>show dvmrp interfaces</td>
<td>Get DVMRP interfaces information</td>
</tr>
<tr>
<td>show dvmrp neighbors</td>
<td>Display DVMRP neighbors</td>
</tr>
<tr>
<td>show dvmrp prefix</td>
<td>Get DVMRP prefix information</td>
</tr>
<tr>
<td>show dvmrp prunes</td>
<td>Display DVMRP prunes</td>
</tr>
<tr>
<td>show dynamic-profile</td>
<td>Display dynamic-profile</td>
</tr>
<tr>
<td>show dynamic-profile session</td>
<td>Get dynamic-profile session information</td>
</tr>
<tr>
<td>show dynamic-tunnels</td>
<td>Display dynamic-tunnels</td>
</tr>
<tr>
<td>show dynamic-tunnels database</td>
<td>Get dynamic-tunnels database information</td>
</tr>
<tr>
<td>show ethernet-switching mac-learning-log</td>
<td>Display Ethernet Switching MAC learning log</td>
</tr>
<tr>
<td>show ethernet-switching mac-notification</td>
<td>Get Ethernet Switching MAC notification</td>
</tr>
<tr>
<td>show ethernet-switching flood next-hops</td>
<td>Display Ethernet Switching Flood next-hops</td>
</tr>
<tr>
<td>show ethernet-switching flood next-hops satellite</td>
<td>Get Ethernet Switching Flood next-hops satellite</td>
</tr>
<tr>
<td>show ethernet-switching flood satellite</td>
<td>Display Ethernet Switching Flood satellite</td>
</tr>
<tr>
<td>show ethernet-switching nh-learn-entity</td>
<td>Display Ethernet Switching NH-learn-entity</td>
</tr>
<tr>
<td>show ethernet-switching redundancy-groups</td>
<td>Display Ethernet Switching Redundancy-groups</td>
</tr>
<tr>
<td>show ethernet-switching satellite</td>
<td>Display Ethernet Switching Satellite</td>
</tr>
<tr>
<td>show ethernet-switching satellite device</td>
<td>Get Ethernet Switching Satellite Device</td>
</tr>
<tr>
<td>show ethernet-switching satellite events</td>
<td>Display Ethernet Switching Satellite Events</td>
</tr>
<tr>
<td>show ethernet-switching satellite logging</td>
<td>Display Ethernet Switching Satellite Logging</td>
</tr>
<tr>
<td>show ethernet-switching satellite summary</td>
<td>Get Ethernet Switching Satellite Summary</td>
</tr>
<tr>
<td>show ethernet-switching table satellite</td>
<td>Display Ethernet Switching Table Satellite</td>
</tr>
<tr>
<td>show ethernet-switching bridge-summary</td>
<td>Get Ethernet Switching Bridge Summary</td>
</tr>
<tr>
<td>show ethernet-switching bridge-mac-table</td>
<td>Get Ethernet Switching Bridge MAC Table</td>
</tr>
</tbody>
</table>
show ethernet-switching vxlan-tunnel-end-point esi
<get-ethernet-switching-vxlan-esi-info>
show ethernet-switching vxlan-tunnel-end-point remote
<get-ethernet-switching-vxlan-rvtep-info>
show ethernet-switching vxlan-tunnel-end-point remote esi
<get-ethernet-switching-vxlan-esi-info>
show ethernet-switching vxlan-tunnel-end-point remote vtep-source-interface
<get-ethernet-switching-vxlan-remote-svtep-ip-information>
show ethernet-switching vxlan-tunnel-end-point source ip
<get-ethernet-switching-vxlan-svtep-ip-information>
show ephemeral-configuration
show esis
show esis adjacency
<get-esis-adjacency-information>
show esis interface
<get-esis-interface-information>
show esis statistics
<get-esis-statistics-information>
show event-options
show event-options event-scripts
show event-options event-scripts policies
<get-event-scripts-policies>
<get-event-summary>
show evpn
show evpn arp-table
<get-evpn-arp-table>
show evpn flood
<get-evpn-flood-information>
show evpn flood event-queue
<get-evpn-event-queue-information>
show evpn flood route
show evpn flood route all-ce-flood
<get-evpn-all-ce-flood-route-information>
show evpn flood route all-flood
<get-evpn-all-flood-route-information>
show evpn flood route alt-root-flood
<get-evpn-alt-root-flood-route-information>
show evpn flood route ce-flood
<get-evpn-ce-flood-route-information>
show evpn flood route mlp-flood
<get-evpn-mlp-flood-route-information>
show evpn flood route re-flood
<get-mspinfo-uptime>
show extension-provider system virtual-memory
<get-core-key-list>
<get-fabric-summary-information>
<get-key-vg-binding>
<get-mac-ip-binding-information>
<get-mc-ccpc-cache-ccpc-select>
<get-mc-ccpc-cache-root-candidates>
<get-mc-ccpc-cache-spf>
<get-mc-ccpc-src-mod-filters>
<get-mc-edge-cache-ccpc-select>
<get-mc-edge-map-to-key-binding>
<get-mc-edge-key-to-map-binding>
<get-mc-edge-vg-portmap>
<get-mc-nsf>
<get-mc-root-cache-trunk>
<get-mc-root-key-to-map-binding>
<get-layer2-group-membership-entries>
<get-layer3-group-membership-entries>
<get-layer3-multicast-pending-routes>
<get-layer3-multicast-receivers>
<get-mc-root-map-to-key-binding>
<get-mc-root-vg-pfemap>
<get-fabric-multicast-statistics>
<get-mc-vccpdf-adjacency-database>
<get-mspinfo-virtual-memory>
get-fabric-statistics
get-fabric-summary-information
<get-vlan-domain-map-information>
show fabric multicast dirty-key-info
<get-mc-dirty-key-info>
show fabric multicast edge corekey-ifls-filters
<get-mc-edge-corekey-ifls-filters>
show fabric multicast edge ine-ifls-filters
<get-mc-edge-ine-ifls-filters>
show fabric multicast edge src-mod-filters
<get-mc-edge-src-mod-filters>
show fabric multicast graph
show fabric multicast graph core-tree
<get-fabric-multicast-graph>
show fabric multicast steal-key-info
<get-mc-steal-key-info>
show forwarding-options
show forwarding-options enhanced-hash-key
show forwarding-options enhanced-hash-key fpc
show forwarding-options hyper-mode
  <get forwarding-options hyper-mode>
show forwarding-options load-balance
show forwarding-options next-hop-group
  <get-forwarding-options-next-hop-group>
show forwarding-options port-mirroring
  <get-forwarding-options-port-mirroring>
show helper
show helper statistics
  <get-helper-statistics-information>
show hfrr
show hfrr profiles
show iccp
  <get-inter-chassis-control-protocol-information>
show igmp
show igmp group
  <get-igmp-group-information>
show igmp interface
  <get-igmp-interface-information>
show igmp output-group
  <get-igmp-output-group-information>
show igmp snooping
show igmp snooping interface
  <get-igmp-snooping-interface-information>
show igmp snooping interface bridge-domain
  <get-igmp-snooping-bridge-domain-interface>
show igmp snooping membership
  <get-igmp-snooping-membership-information>
show igmp snooping membership bridge-domain
show igmp snooping options
  <get-igmp-snooping-options-information>
show igmp snooping options
get-igmp-snooping-options-information
show igmp snooping statistics
  <get-igmp-snooping-statistics-information>
show igmp snooping statistics bridge-domain
  <get-igmp-snooping-bridge-domain-membership>
show igmp statistics
  <get-igmp-statistics-information>
show ike
show ike security-associations
    <get-ike-security-associations-information>

show ilmi
<get-ilmi-information>
show ilmi interface
<get-ilmi-interface-information>
show ilmi statistics
<get-ilmi-statistics>
show ingress-replication
    <get-ingress-replication-information>
show interfaces
    <get-interface-information>
show interfaces anchor-group
show interfaces controller
<get-interface-controller-information>
show interfaces destination-class
    <get-destination-class-statistics>

show interfaces destination-class all
<get-all-destination-class-statistics>
show interfaces diagnostics
show interfaces diagnostics optics
    <get-interface-optics-diagnostics-information>
show interfaces diagnostics optics satellite
<show-interface-optics-diagnostics-satellite>
show interfaces distribution-list
<get-distribution-list-information>

show interfaces far-end-interval
    <show-interfaces-far-end-interval>
show interfaces filters
    <get-interface-filter-information>

show interfaces forwarding-class-counters
<get-interface-fc-counters-information>

show interfaces interface-set
<get-interface-set-information>
show interfaces interface-set queue
<get-interface-set-queue-information>

show interfaces interval
  <show-interfaces-interval>
show interfaces lib-clients
  <get-dcd-lib-client-data>
show interfaces load-balancing
  <interface-load-balancing>
show interfaces mac-database
  <get-mac-database>

show interfaces mc-ae
  <get-mc-ae-interface-information>
show interfaces mc-ae revertive-info
  <get-mc-ae-revertive-information>
show interfaces policers
  <get-interface-policer-information>

show interfaces queue
  <get-interface-queue-information>

show interfaces redundancy
  <get-redundancy-status>
show interfaces redundancy detail
  <get-redundancy-status-details>
show interfaces routing
show interfaces source-class
  <get-source-class-statistics>

show interfaces source-class all
  <get-all-source-class-statistics>
show interfaces targeting
  <get-targeting-information>
show interfaces transport
  <get-interface-transport-information>
show interfaces transport optics
  <get-interface-transport-optics-information>
show interfaces transport optics interval
  <get-interface-transport-optics-interval-information>
show interfaces voq
  <get-interface-voq-information>
show ipsec
show ipsec redundancy
show ipsec redundancy interface
  <get-ipsec-pic-redundancy-information>

show ipsec redundancy security-associations
  <get-ipsec-tunnel-redundancy-information>

show ipsec security-associations
  <get-security-associations-information>

show ipv6
show ipv6 neighbors
  <get-ipv6-nd-information>

show ipv6 router-advertisement
  <get-ipv6-ra-information>

show isis
show isis adjacency
  <get-isis-adjacency-information>

show isis authentication
  <get-isis-authentication-information>

show isis backup
show isis backup coverage
  <get-isis-backup-coverage-information>

show isis backup label-switched-path
  <get-isis-backup-lsp-information>

show isis backup spf
show isis backup spf results
  <get-isis-backup-spf-results-information>
show isis bgp-orr
  <get-isis-bgporr-information>

show isis context-identifier
  <get-isis-context-identifier-information>

show isis context-identifier identifier
<get-isis-context-identifier-origin-information>
show isis database
   <get-isis-database-information>

show isis hostname
   <get-isis-hostname-information>

show isis interface
   <get-isis-interface-information>
show isis interface-group
   <get-isis-interface-group-information>
show isis layer2-map
   <get-isis-layer2-map-information>

show isis overview
   <get-isis-overview-information>

show isis route
   <get-isis-route-information>

show isis spf
show isis spf brief
   <get-isis-spf-results-brief-information>

show isis spf log
   <get-isis-spf-log-information>

show isis spf results
   <get-isis-spf-results-information>

show isis statistics
   <get-isis-statistics-information>

show 12-learning
show 12-learning backbone-instance
   <get-12-learning-backbone-instance>
show 12-learning evpn
show 12-learning evpn arp-statistics
   <get-evpn-arp-statistics>
show 12-learning evpn arp-statistics interface
   <get-evpn-arp-statistics-interface>
show 12-learning evpn nd-statistics
<get-evpn-nd-statistics>
show 12-learning evpn nd-statistics interface
<get-evpn-nd-statistics-interface>
show 12-learning global-information
<get-12-learning-global-information>
show 12-learning global-mac-count
<get-12-learning-global-mac-count>
show 12-learning instance
<get-12-learning-routing-instances>
show 12-learning interface
<get-12-learning-interface-information>
show 12-learning mac-move-buffer
<get-12-learning-mac-move-buffer-information>
show 12-learning provider-instance
<get-12-learning-provider-instance>
show 12-learning redundancy-groups
<get-12-learning-redundancy-groups>
show 12-learning remote-backbone-edge-bridges
<get-12-learning-remote-backbone-edge-bridges>
show 12-learning vxlan-tunnel-end-point
show 12-learning vxlan-tunnel-end-point esi
<get-12-learning-vxlan-esi-info>
show 12-learning vxlan-tunnel-end-point remote
<get-12-learning-vxlan-rvtep-info>
show 12-learning vxlan-tunnel-end-point remote ip
<get-12-learning-vxlan-rvtep-ip-information>
show 12-learning vxlan-tunnel-end-point remote mac-table
<get-12-learning-vxlan-rvtep-mactable-information>
show 12-learning vxlan-tunnel-end-point remote vtep-source-interface
<get-12-learning-vxlan-remote-svtep-ip-information>
show 12-learning vxlan-tunnel-end-point source
<get-12-learning-vxlan-svtep-info>
show 12-learning vxlan-tunnel-end-point source ip
<get-12-learning-vxlan-svtep-ip-information>
show 12circuit
show 12circuit auto-sensing
<get-12ckt-pw-auto-sensing-information>
show 12circuit connections
<get-12ckt-connection-information>

show 12cpd
show 12cpd task
<get-12cpd-task-information>
show 12cpd task io
  <get-12cpd-tasks-io-statistics>
show 12cpd task memory
  <get-12cpd-task-memory>
show 12cpd task replication
  <get-12cpd-replication-information>
show 12vpn
show 12vpn connections
  <get-12vpn-connection-information>

show lacp
show lacp interfaces
  <get-lacp-interface-information>
show lacp statistics
show lacp statistics interfaces
  <get-lacp-interface-statistics>
show lacp timeouts
show ldp
show ldp database
  <get-ldp-database-information>

show ldp fec-filters
  <get-ldp-fec-filters-information>

show ldp interface
  <get-ldp-interface-information>

show ldp neighbor
  <get-ldp-neighbor-information>

show ldp oam
  <get-ldp-oam-information>
show ldp overview
  <get-ldp-overview-information>
show ldp p2mp
show ldp p2mp fec
  <get-ldp-p2mp-fec-information>
show ldp p2mp path
  <get-ldp-p2mp-path-information>
show ldp p2mp tunnel
  <get-ldp-p2mp-tunnel-information>
show ldp path
<get-ldp-path-information>

show ldp rib-groups
<get-ldp-rib-groups-information>
show ldp route
<get-ldp-route-information>

show ldp session
<get-ldp-session-information>

show ldp statistics
<get-ldp-statistics-information>

show ldp traffic-statistics
<get-ldp-traffic-statistics-information>

show link-management
<get-lm-information>

show link-management peer
<get-lm-peer-information>

show link-management routing
<get-lm-routing-information>

show link-management routing peer
<get-lm-routing-peer-information>

show link-management routing resource
<get-lm-routing-resource-information>

show link-management routing te-link
<get-lm-routing-te-link-information>

show lldp
<get-lldp-information>

show lldp detail
<get-lldp-information-detail>

show lldp local-information
<get-lldp-local-info>
show lldp neighbors
    <get-lldp-neighbors-information>

show lldp neighbors interface
    <get-lldp-interface-neighbors>
show lldp remote-global-statistics
    <get-lldp-remote-global-statistics>

show lldp statistics
    <get-lldp-statistics-information>

show lldp statistics interface
    <get-lldp-interface-statistics>
show loop-detect
show loop-detect interface
    <get-loop-detect-interface-information>
show loop-detect statistics
show loop-detect statistics interface
    <get-loop-detect-interface-statistics-information>
show link-management statistics
    <get-lm-statistics-information>

show link-management statistics peer
    <get-lm-peer-statistics>

show link-management te-link
    <get-lm-te-link-information>

show mac-rewrite
show mac-rewrite interface
    <get-mac-rewrite-interface-information>
show mld
show mld group
    <get-mld-group-information>

show mld interface
    <get-mld-interface-information>

show mld output-group
    <get-mld-output-group-information>
show mld snooping
show mld snooping interface
<get-mld-snooping-interface-information>
show mld snooping interface bridge-domain
<get-mld-snooping-bridge-domain-interface>
show mld snooping interface vlan
<get-mld-snooping-vlan-interface>
show mld snooping membership
<get-mld-snooping-membership-information>
show mld snooping membership bridge-domain
<get-mld-snooping-bridge-domain-membership>
show mld snooping membership vlan
<get-mld-snooping-vlan-membership>
show mld snooping statistics
<get-mld-snooping-statistics-information>
show mld snooping statistics bridge-domain
<get-mld-snooping-bridge-domain-statistics>
show mld snooping statistics vlan
<get-mld-snooping-vlan-statistics>
show mld statistics
<get-mld-statistics-information>
show mobile-ip
show mobile-ip home-agent
show mobile-ip home-agent binding
<get-mip-binding-information>
show mobile-ip home-agent binding ip-address
<get-ip-mip-binding-information>
show mobile-ip home-agent binding nai
<get-nai-mip-binding-information>
show mobile-ip home-agent binding summary
<get-summary-mip-binding-information>
show mobile-ip home-agent interface
<get-mip-ha-interface-information>
show mobile-ip home-agent overview
<get-mip-ha-overview-information>
show mobile-ip home-agent traffic
    <get-mip-ha-traffic-information>

show mobile-ip home-agent virtual-network
    <get-mip-ha-virtual-network-information>

show mobile-ip tunnel
    <get-mip-tunnel-information>
show mobile-ip wimax
show mobile-ip wimax release
    <get-mip-wimax-release-information>

show mpls
show mpls abstract-hop-membership
    <get-mpls-abstract-hop-membership-information>
show mpls admin-groups
    <get-mpls-admin-group-information>

show mpls admin-groups-extended
    <get-mpls-admin-group-extended-information>
show mpls association
show mpls association iif
    <get-mpls-association-iif-information>
show mpls association oif
    <get-mpls-association-oif-information>
show mpls association path
    <get-mpls-association-path-information>
show mpls call-admission-control
    <get-mpls-call-admission-control-information>

show mpls context-identifier
    <get-mpls-context-identifier-information>
show mpls correlation
show mpls correlation label
    <get-mpls-correlation-label-information>
show mpls correlation nexthop-id
    <get-mpls-correlation-nexthop-information>

show network-access address-assignment preserved
    <get-address-assignment-preserved-table>
show network-access domain-map
show network-access domain-map statistics
<get-domain-map-statistics>
show mpls cspf
  <get-mpls-cspf-information>

show mpls diffserv-te
  <get-mpls-diffserv-te-information>
show mpls egress-protection
show mpls interface
  <get-mpls-interface-information>
show mpls label
  <get mpls-label-space>
show mpls label usage
  <get mpls-label-space-usage>

show mpls lsp
  <get-mpls-lsp-information>
show mpls lsp abstract-computation
  <get-mpls-lsp-abstract-computation>

show mpls lsp autobandwidth
  <get-mpls-lsp-autobandwidth>
show mpls srlg
  <get-mpls-srlg-information>
show oam ethernet fnp
show oam ethernet fnp interface
show oam ethernet fnp messages
show oam ethernet fnp status
  <get-fnp-status>
show mpls lsp defaults
  <get-mpls-lsp-defaults-information>

show mpls path
  <get-mpls-path-information>

show mpls static-lsp
  <get-mpls-static-lsp-information>
show mpls traceroute
show mpls traceroute database
show mpls traceroute database ldp
  <get-mpls-traceroute-database-ldp>
show msdp
  <get-msdp-information>
show msdp source
  <get-msdp-source-information>

show msdp source-active
  <get-msdp-source-active-information>

show msdp statistics
  <get-msdp-statistics-information>
show multi-chassis
show multi-chassis mc-lag
show multi-chassis mc-lag configuration-consistency
  <get-mclag-config-consistency-information>
show multi-chassis mc-lag configuration-consistency global-config
  <get-mclag-global-config-consistency-information>
show multi-chassis mc-lag configuration-consistency icl-config
  <get-mclag-icl-config-consistency-information>
show multi-chassis mc-lag configuration-consistency
list-of-parameters
  <get-mclag-config-consistency-information-params>
show multi-chassis mc-lag configuration-consistency mcae-config
get-mclag-config-consistency-information-mcae
show multi-chassis mc-lag configuration-consistency vlan-config
  <get-mclag-vlan-config-consistency-information>
show multi-chassis mc-lag configuration-consistency vrrp-config
  <get-mclag-vrrp-config-consistency-information>
show multicast
show multicast backup-pe-groups
  <get-multicast-backup-pe-groups-information>
show multicast backup-pe-groups address
  <get-multicast-backup-pe-address-information>
show multicast backup-pe-groups group
  <get-multicast-backup-pe-group-information>
show multicast ecid-mapping
show multicast ecid-mapping satellite
  <get-satellite-control-ecid>
show multicast flow-map
  <get-multicast-flow-maps-information>
show multicast interface
  <get-multicast-interface-information>
show multicast next-hops
  <get-multicast-next-hops-information>
show multicast next-hops satellite
  <get-satellite-control-next-hop>

show multicast pim-to-igmp-proxy
  <get-multicast-pim-to-igmp-proxy-information>

show multicast pim-to-mld-proxy
  <get-multicast-pim-to-mld-proxy-information>

show multicast route
  <get-multicast-route-information>

show multicast rpf
  <get-multicast-rpf-information>

show multicast scope
  <get-multicast-scope-information>

show multicast sessions
  <get-multicast-sessions-information>

show multicast snooping
show multicast snooping next-hops
  <get-multicast-snooping-next-hops-information>

show multicast snooping next-hops satellite
  <get-satellite-control-indirect-next-hop>
show multicast snooping route
  <get-multicast-snooping-route-information>
show multicast snooping route satellite
get-satellite-control-multicast

show multicast statistics
  <get-multicast-statistics-information>
show multicast statistics satellite
  <get-satellite-control-statistics>
show multicast summary
show multicast summary satellite
  <get-satellite-control-summary>
show multicast usage
  <get-multicast-usage-information>

show mvpn
show mvpn c-multicast
<get-mvpn-c-multicasti-route>
show mvpn instance
  <get-mvpn-instance-information>

show mvpn neighbor
<get-mvpn-neighbor-information>
show mvpn suppressed
get-mvpn-suppressed-information
show mvrp
  <get-mvrp-information>

show mvrp applicant-state
  <get-mvrp-applicant-information>

show mvrp dynamic-vlan-memberships
  <get-mvrp-dynamic-vlan-memberships>

show mvrp interface
  <get-mvrp-interface-information>

show mvrp registration-state
  <get-mvrp-registration-state>

show mvrp statistics
  <get-mvrp-interface-statistics>

show network-access
show network-access aaa
show network-access aaa radius-servers
<get-radius-servers-table>
show network-access aaa statistics
  <get-aaa-module-statistics>

show network-access aaa statistics address-assignment
show network-access aaa statistics address-assignment client
<get-address-assignment-client-statistics>
show network-access aaa statistics address-assignment pool
<get-address-assignment-pool-statistics>
show network-access aaa subscribers
<get-aaa-subscriber-table>
show network-access aaa subscribers session-id
show network-access aaa subscribers statistics
<get-aaa-subscriber-statistics>
show network-access aaa terminate-code
<get-aaa-terminate-code>
show network-access aaa terminate-code aaa
<get-aaa-terminate-code-aaa>
show network-access aaa terminate-code dhcp
<get-aaa-terminate-code-dhcp>
show network-access aaa terminate-code 12tp
<get-aaa-terminate-code-12tp>
show network-access aaa terminate-code ppp
<get-aaa-terminate-code-ppp>
show network-access aaa terminate-code reverse
<get-aaa-terminate-code-reverse>
show network-access aaa terminate-code reverse aaa
<get-aaa-terminate-code-reverse-aaa>
show network-access aaa terminate-code reverse dhcp
<get-aaa-terminate-code-reverse-dhcp>
show network-access aaa terminate-code reverse 12tp
<get-aaa-terminate-code-reverse-12tp>
show network-access aaa terminate-code reverse ppp
<get-aaa-terminate-code-reverse-ppp>
show network-access address-assignment
show network-access address-assignment pool
<get-address-assignment-pool-table>
show network-access nasreq
show network-access nasreq statistics
get-nasreq-counters
show network-access ocs
show network-access ocs state
<get-ocs-state-information>
show network-access ocs statistics
<get-ocs-statistics-information>
show network-access pcrf
show network-access pcrf state
 get-pcrf-state-information

show network-access pcrf statistics
 get-pcrf-statistics-information

show network-access requests
show network-access requests pending
 get-authentication-pending-table

show network-access requests statistics
 get-authentication-statistics

show network-access securid-node-secret-file
 get-node-secret-file-table

show nonstop-routing
 get-nonstop-routing-information

show ntp
show ntp associations
show ntp status
show oam
show oam ethernet
show oam ethernet connectivity-fault-management sla-iterator-history
 get-cfm-iterator-history

show oam ethernet connectivity-fault-management
show oam ethernet connectivity-fault-management adjacencies
 get-cfm-adjacency-information

show oam ethernet connectivity-fault-management delay-statistics
 get-cfm-delay-statistics

show oam ethernet connectivity-fault-management forwarding-state
show oam ethernet connectivity-fault-management forwarding-state instance
 get-cfm-forwarding-state-instance-information

show oam ethernet connectivity-fault-management forwarding-state interface
 get-cfm-forwarding-state-interface-information

show oam ethernet connectivity-fault-management interfaces
 get-cfm-interfaces-information

show oam ethernet connectivity-fault-management loss-statistics
 get-cfm-loss-statistics
show oam ethernet connectivity-fault-management mep-database
  <get-cfm-mep-database>

show oam ethernet connectivity-fault-management mep-statistics
  <get-cfm-mep-statistics>

show oam ethernet connectivity-fault-management mip
  <get-cfm-mip-information>

show oam ethernet connectivity-fault-management path-database
  <get-cfm-linktrace-path-database>

show oam ethernet connectivity-fault-management policer
  <get-evc-information>

show oam ethernet connectivity-fault-management sla-iterator-statistics
  <get-cfm-iterator-statistics>

show oam ethernet evc
  <get-evc-infromation>

show oam ethernet link-fault-management
  <get-lfmd-information>

show oam ethernet lmi
  <get-elmi-information>

show oam ethernet lmi statistics
  <get-elmi-statistics>

show openflow
show openflow capability
show openflow controller
show openflow filters
show openflow flows
show openflow interfaces
show openflow statistics
show openflow statistics flows
show openflow statistics interfaces
show openflow statistics packet
show openflow statistics packet in
show openflow statistics packet out
show openflow statistics queue
show openflow statistics summary
show openflow statistics tables
show openflow summary
show openflow switch

show ospf
show ospf backup
show ospf backup coverage
  <get-ospf-backup-coverage-information>

show ospf backup lsp
  <get-ospf-backup-lsp-information>

show ospf backup neighbor
  <get-ospf-backup-neighbor-information>

show ospf backup spf
  <get-ospf-backup-spf-information>
show ospf bgp-orr
  <get-ospf-bgporr-information>

show ospf context-identifier
  <get-ospf-context-id-information>

show ospf database
  <get-ospf-database-information>

show ospf interface
  <get-ospf-interface-information>

show ospf io-statistics
  <get-ospf-io-statistics-information>

show ospf log
  <get-ospf-log-information>

show ospf neighbor
  <get-ospf-neighbor-information>

show ospf overview
  <get-ospf-overview-information>

show ospf route
<get-ospf-route-information>

show ospf statistics
   <get-ospf-statistics-information>

show ospf3
show ospf3 backup
show ospf3 backup coverage
   <get-ospf3-backup-coverage-information>

show ospf3 backup lsp
   <get-ospf3-backup-lsp-information>

show ospf3 backup neighbor
   <get-ospf3-backup-neighbor-information>

show ospf3 backup spf
   <get-ospf3-backup-spf-information>
show ospf3 bgp-orr
   <get-ospf3-bgprr-information>

show ospf3 database
   <get-ospf3-database-information>

show ospf3 interface
   <get-ospf3-interface-information>

show ospf3 io-statistics
   <get-ospf3-io-statistics-information>

show ospf3 log
   <get-ospf3-log-information>

show ospf3 neighbor
   <get-ospf3-neighbor-information>

show ospf3 overview
   <get-ospf3-overview-information>

show ospf3 route
   <get-ospf3-route-information>
show ospf3 statistics
  <get-ospf3-statistics-information>
show overlay
  <get-cloud-analytics-overlay-information>
show overlay vxlan
  <get-cloud-analytics-overlay-vxlan-information>
show overlay vxlan vni
  <get-application-monitor-overlay-vxlan-vni-information>
show overlay vxlan vtep
  <get-application-monitor-overlay-vxlan-vtep-information>
show ovsdb
show ovsdb commit
show ovsdb commit failures
  <get-ovsdb-commit-failure-information>
show ovsdb tunnels
  <get-ovsdb-tunnels-information>
show ovsdb virtual-tunnel-end-point
  <get-ovsdb-vtep-information>
show passive-monitoring
  <get-passive-monitoring-information>
show passive-monitoring error
  <get-passive-monitoring-error-information>
show passive-monitoring flow
  <get-passive-monitoring-flow-information>
show passive-monitoring memory
  <get-passive-monitoring-memory-information>
show passive-monitoring status
  <get-passive-monitoring-status-information>
show passive-monitoring usage
  <get-passive-monitoring-usage-information>
show path-computation-client
show path-computation-client active-pce
show path-computation-client lsp-retry-pending
  <get-path-computation-client-lsp-retry-pending-information>
show path-computation-client statistics
show performance-monitoring
show performance-monitoring mpls
show performance-monitoring mpls lsp
<get-pm-mpls-lsp-information>
show pfe
show pfe cfec
show pfe data
<get-pfe-data>
show pfe feb
show pfe filter
show pfe filter hw
show pfe filter hw summary
show pfe fpn
show pfe fwdd
show pfe lcc
show pfe next-hop
show pfe pfem
show pfe pfem detail
show pfe pfem extensive
show pfe route
show pfe route clnp
show pfe route clnp table
show pfe route inet6
show pfe route inet6 hw
show pfe route inet6 hw host
show pfe route inet6 hw lpm
show pfe route inet6 hw multicast
show pfe route inet6 table
show pfe route ip
show pfe route ip table
show pfe route iso
show pfe route iso table
show pfe scb
show pfe sfm
show pfe sbb
show pfe statistics
show pfe statistics exceptions
show pfe statistics fabric
show pfe statistics ip
show pfe route ip hw
show pfe route ip hw host
show pfe route ip hw lpm
show pfe route ip hw multicast
show pfe route summary
show pfe route summary hw
show pfe statistics ip6
show pfe statistics traffic
   <get-pfe-statistics>
show pfe statistics traffic bandwidth
   <get-pfe-traffic-statistics-bandwidth>

show pfe statistics traffic cpu
show pfe statistics traffic cpu fpe
show pfe statistics traffic detail
   <get-pfe-traffic-statistics>
show pfe statistics traffic egress-queues
show pfe statistics traffic egress-queues fpc
show pfe statistics traffic multicast
show pfe statistics traffic multicast fpc
show pfe statistics traffic protocol
show pfe tcam
show pfe tcam app
   <get-pfe-tcam-app-list>
show pfe tcam app bd-dtag-validate
   <get-pfe-tcam-app-list-bd-dtag-validate>
show pfe tcam app bd-dtag-validate detail
show pfe tcam app bd-dtag-validate list-related-apps
show pfe tcam app bd-dtag-validate list-shared-apps
show pfe tcam app bd-dtag-validate shared-usage
show pfe tcam app bd-dtag-validate shared-usage detail
show pfe tcam app bd-tpid-swap
   <get-pfe-tcam-app-list-bd-tpid-swap>
show pfe tcam app bd-tpid-swap detail
show pfe tcam app bd-tpid-swap list-related-apps
show pfe tcam app bd-tpid-swap list-shared-apps
show pfe tcam app bd-tpid-swap shared-usage
show pfe tcam app bd-tpid-swap shared-usage detail
show pfe tcam app cfm-bd-filter
   <get-pfe-tcam-app-list-cfm-bd-filter>
show pfe tcam app cfm-bd-filter detail
show pfe tcam app cfm-bd-filter list-related-apps
show pfe tcam app cfm-bd-filter list-shared-apps
show pfe tcam app cfm-bd-filter shared-usage
show pfe tcam app cfm-bd-filter shared-usage detail
show pfe tcam app cfm-filter
<get-pfe-tcam-app-list-cfm-filter>
show pfe tcam app cfm-filter list-related-apps
show pfe tcam app cfm-filter list-shared-apps
show pfe tcam app cfm-filter shared-usage
show pfe tcam app cfm-filter shared-usage detail
show pfe tcam app cfm-vpls-filter
<get-pfe-tcam-app-list-cfm-vpls-filter>
show pfe tcam app cfm-vpls-filter detail
show pfe tcam app cfm-vpls-filter list-related-apps
show pfe tcam app cfm-vpls-filter list-shared-apps
show pfe tcam app cfm-vpls-filter shared-usage
show pfe tcam app cfm-vpls-filter shared-usage detail
show pfe tcam app cfm-vpls-ifl-filter
<get-pfe-tcam-app-list-cfm-vpls-ifl-filter>
show pfe tcam app cfm-vpls-ifl-filter detail
show pfe tcam app cfm-vpls-ifl-filter list-related-apps
show pfe tcam app cfm-vpls-ifl-filter list-shared-apps
show pfe tcam app cfm-vpls-ifl-filter shared-usage
show pfe tcam app cfm-vpls-ifl-filter shared-usage detail
show pfe tcam app cos-fc
<get-pfe-tcam-app-list-cos-fc>
show pfe tcam app cos-fc detail
show pfe tcam app cos-fc list-related-apps
show pfe tcam app cos-fc list-shared-apps
show pfe tcam app cos-fc shared-usage
show pfe tcam app cos-fc shared-usage detail
show pfe tcam app fw-ccc-in
<get-pfe-tcam-app-list-fw-ccc-in>
show pfe tcam app fw-ccc-in detail
show pfe tcam app fw-ccc-in list-related-apps
show pfe tcam app fw-ccc-in list-shared-apps
show pfe tcam app fw-ccc-in shared-usage
show pfe tcam app fw-ccc-in shared-usage detail
show pfe tcam app fw-family-out
<get-pfe-tcam-app-list-fw-family-out>
show pfe tcam app fw-family-out detail
show pfe tcam app fw-family-out list-related-apps
show pfe tcam app fw-family-out list-shared-apps
show pfe tcam app fw-family-out shared-usage
show pfe tcam app fw-family-out shared-usage detail
show pfe tcam app fw-fbf
<get-pfe-tcam-app-list-fw-fbf>
show pfe tcam app fw-fbf detail
show pfe tcam app fw-fbf list-related-apps
show pfe tcam app fw-fbf list-shared-apps
show pfe tcam app fw-fbf shared-usage
show pfe tcam app fw-fbf shared-usage detail
  show pfe tcam app fw-fbf-inet6
  <get-pfe-tcam-app-list-fw-fbf-inet6>
show pfe tcam app fw-fbf-inet6 detail
show pfe tcam app fw-fbf-inet6 list-related-apps
show pfe tcam app fw-fbf-inet6 list-shared-apps
show pfe tcam app fw-fbf-inet6 shared-usage
show pfe tcam app fw-fbf-inet6 shared-usage detail
show pfe tcam app fw-ifl-in
  <get-pfe-tcam-app-list-fw-ifl-in>
show pfe tcam app fw-ifl-in detail
show pfe tcam app fw-ifl-in list-related-apps
show pfe tcam app fw-ifl-in list-shared-apps
show pfe tcam app fw-ifl-in shared-usage
show pfe tcam app fw-ifl-in shared-usage detail
show pfe tcam app fw-ifl-out
  <get-pfe-tcam-app-list-fw-ifl-out>
show pfe tcam app fw-ifl-out detail
show pfe tcam app fw-ifl-out list-related-apps
show pfe tcam app fw-ifl-out list-shared-apps
show pfe tcam app fw-ifl-out shared-usage
show pfe tcam app fw-ifl-out shared-usage detail
show pfe tcam app fw-inet-ftf
  <get-pfe-tcam-app-list-fw-inet-ftf>
show pfe tcam app fw-inet-ftf detail
show pfe tcam app fw-inet-ftf list-related-apps
show pfe tcam app fw-inet-ftf list-shared-apps
show pfe tcam app fw-inet-ftf shared-usage
show pfe tcam app fw-inet-ftf shared-usage detail
show pfe tcam app fw-inet-in
  <get-pfe-tcam-app-list-fw-inet-in>
show pfe tcam app fw-inet-in detail
show pfe tcam app fw-inet-in list-related-apps
show pfe tcam app fw-inet-in list-shared-apps
show pfe tcam app fw-inet-in shared-usage
show pfe tcam app fw-inet-in shared-usage detail
show pfe tcam app fw-inet-pm
  <get-pfe-tcam-app-list-fw-inet-pm>
show pfe tcam app fw-inet-pm detail
show pfe tcam app fw-inet-pm list-related-apps
show pfe tcam app fw-inet-pm list-shared-apps
show pfe tcam app fw-inet-pm shared-usage
show pfe tcam app fw-inet-pm shared-usage detail
show pfe tcam app fw-inet-rpf
<get-pfe-tcam-app-list-fw-inet-rpf>
show pfe tcam app fw-inet-rpf detail
show pfe tcam app fw-inet-rpf list-related-apps
show pfe tcam app fw-inet-rpf list-shared-apps
show pfe tcam app fw-inet-rpf shared-usage
show pfe tcam app fw-inet-rpf shared-usage detail
show pfe tcam app fw-inet6-family-out
<get-pfe-tcam-app-list-fw-inet6-family-out>
show pfe tcam app fw-inet6-family-out detail
show pfe tcam app fw-inet6-family-out list-related-apps
show pfe tcam app fw-inet6-family-out list-shared-apps
show pfe tcam app fw-inet6-family-out shared-usage
show pfe tcam app fw-inet6-family-out shared-usage detail
show pfe tcam app fw-inet6-ftf
<get-pfe-tcam-app-list-fw-inet6-ftf>
show pfe tcam app fw-inet6-ftf detail
show pfe tcam app fw-inet6-ftf list-related-apps
show pfe tcam app fw-inet6-ftf list-shared-apps
show pfe tcam app fw-inet6-ftf shared-usage
show pfe tcam app fw-inet6-ftf shared-usage detail
show pfe tcam app fw-inet6-in
<get-pfe-tcam-app-list-fw-inet6-in>
show pfe tcam app fw-inet6-in detail
show pfe tcam app fw-inet6-in list-related-apps
show pfe tcam app fw-inet6-in list-shared-apps
show pfe tcam app fw-inet6-in shared-usage
show pfe tcam app fw-inet6-in shared-usage detail
show pfe tcam app fw-inet6-rpf
<get-pfe-tcam-app-list-fw-inet6-rpf>
show pfe tcam app fw-inet6-rpf detail
show pfe tcam app fw-inet6-rpf list-related-apps
show pfe tcam app fw-inet6-rpf list-shared-apps
show pfe tcam app fw-inet6-rpf shared-usage
show pfe tcam app fw-inet6-rpf shared-usage detail
show pfe tcam app fw-12-in
<get-pfe-tcam-app-list-fw-12-in>
show pfe tcam app fw-l2-in detail
show pfe tcam app fw-l2-in list-related-apps
show pfe tcam app fw-l2-in list-shared-apps
show pfe tcam app fw-l2-in shared-usage
show pfe tcam app fw-l2-in shared-usage detail
show pfe tcam app fw-mpls-in
<get-pfe-tcam-app-list-fw-mpls-in>
show pfe tcam app fw-mpls-in detail
show pfe tcam app fw-mpls-in list-related-apps
show pfe tcam app fw-mpls-in list-shared-apps
show pfe tcam app fw-mpls-in shared-usage
show pfe tcam app fw-mpls-in shared-usage detail
show pfe tcam app fw-semantics
<get-pfe-tcam-app-list-fw-semantics>
show pfe tcam app fw-semantics detail
show pfe tcam app fw-semantics list-related-apps
show pfe tcam app fw-semantics list-shared-apps
show pfe tcam app fw-semantics shared-usage
show pfe tcam app fw-semantics shared-usage detail
show pfe tcam app fw-vpls-in
<get-pfe-tcam-app-list-fw-vpls-in>
show pfe tcam app fw-vpls-in detail
show pfe tcam app fw-vpls-in list-related-apps
show pfe tcam app fw-vpls-in list-shared-apps
show pfe tcam app fw-vpls-in shared-usage
show pfe tcam app fw-vpls-in shared-usage detail
show pfe tcam app gr-ifl-stats-egr
<get-pfe-tcam-app-list-gr-ifl-statistics-egr>
show pfe tcam app gr-ifl-stats-egr detail
show pfe tcam app gr-ifl-stats-egr list-related-apps
show pfe tcam app gr-ifl-stats-egr list-shared-apps
show pfe tcam app gr-ifl-stats-egr shared-usage
show pfe tcam app gr-ifl-stats-egr shared-usage detail
show pfe tcam app gr-ifl-stats-ing
<get-pfe-tcam-app-list-gr-ifl-statistics-ing>
show pfe tcam app gr-ifl-stats-ing detail
show pfe tcam app gr-ifl-stats-ing list-related-apps
show pfe tcam app gr-ifl-stats-ing list-shared-apps
show pfe tcam app gr-ifl-stats-ing shared-usage
show pfe tcam app gr-ifl-stats-ing shared-usage detail
show pfe tcam app gr-ifl-stats-preing
<get-pfe-tcam-app-list-gr-ifl-statistics-preing>
show pfe tcam app gr-ifl-stats-preing detail
show pfe tcam app gr-ifl-stats-preing list-related-apps
show pfe tcam app gr-ifl-stats-preing list-shared-apps
show pfe tcam app gr-ifl-stats-preing shared-usage
show pfe tcam app gr-ifl-stats-preing shared-usage detail
show pfe tcam app ifd-src-mac-fil
<get-pfe-tcam-app-list-ifd-src-mac-fil>
show pfe tcam app ifd-src-mac-fil detail
show pfe tcam app ifd-src-mac-fil list-related-apps
show pfe tcam app ifd-src-mac-fil list-shared-apps
show pfe tcam app ifd-src-mac-fil shared-usage
show pfe tcam app ifd-src-mac-fil shared-usage detail
show pfe tcam app ifl-statistics-in
<get-pfe-tcam-app-list-ifl-statistics-in>
show pfe tcam app ifl-statistics-in detail
show pfe tcam app ifl-statistics-in list-related-apps
show pfe tcam app ifl-statistics-in list-shared-apps
show pfe tcam app ifl-statistics-in shared-usage
show pfe tcam app ifl-statistics-in shared-usage detail
show pfe tcam app ifl-statistics-out
<get-pfe-tcam-app-list-ifl-statistics-out>
show pfe tcam app ifl-statistics-out detail
show pfe tcam app ifl-statistics-out list-related-apps
show pfe tcam app ifl-statistics-out list-shared-apps
show pfe tcam app ifl-statistics-out shared-usage
show pfe tcam app ifl-statistics-out shared-usage detail
show pfe tcam app ing-out-iff
<get-pfe-tcam-app-list-ing-out-iff>
show pfe tcam app ing-out-iff detail
show pfe tcam app ing-out-iff list-related-apps
show pfe tcam app ing-out-iff list-shared-apps
show pfe tcam app ing-out-iff shared-usage
show pfe tcam app ing-out-iff shared-usage detail
show pfe tcam app ip-mac-val
<get-pfe-tcam-app-list-ip-mac-val>
show pfe tcam app ip-mac-val detail
show pfe tcam app ip-mac-val list-related-apps
show pfe tcam app ip-mac-val list-shared-apps
show pfe tcam app ip-mac-val shared-usage
show pfe tcam app ip-mac-val shared-usage detail
show pfe tcam app ip-mac-val-bcast
<get-pfe-tcam-app-list-ip-mac-val-bcast>
show pfe tcam app ip-mac-val-bcast detail
show pfe tcam app ip-mac-val-bcast list-related-apps
show pfe tcam app ip-mac-val-bcast list-shared-apps
show pfe tcam app ip-mac-val-bcast shared-usage
detail
show pfe tcam app ipsec-reverse-fil
<get-pfe-tcam-app-list-ipsec-reverse-fil>
show pfe tcam app ipsec-reverse-fil detail
show pfe tcam app ipsec-reverse-fil list-related-apps
show pfe tcam app ipsec-reverse-fil list-shared-apps
show pfe tcam app irb-cos-rw
<get-pfe-tcam-app-list-irb-cos-rw>
show pfe tcam app irb-cos-rw detail
show pfe tcam app irb-cos-rw list-related-apps
show pfe tcam app irb-cos-rw list-shared-apps
show pfe tcam app irb-cos-rw shared-usage
detail
show pfe tcam app irb-fixed-cos
<get-pfe-tcam-app-list-irb-fixed-cos>
show pfe tcam app irb-fixed-cos detail
show pfe tcam app irb-fixed-cos list-related-apps
show pfe tcam app irb-fixed-cos list-shared-apps
show pfe tcam app irb-fixed-cos shared-usage
detail
show pfe tcam app irb-inet6-fil
<get-pfe-tcam-app-list-irb-inet6-fil>
show pfe tcam app irb-inet6-fil detail
show pfe tcam app irb-inet6-fil list-related-apps
show pfe tcam app irb-inet6-fil list-shared-apps
show pfe tcam app irb-inet6-fil shared-usage
detail
show pfe tcam app lfm-802.3ah-in
<get-pfe-tcam-app-list-lfm-802.3ah-in>
show pfe tcam app lfm-802.3ah-in list-related-apps
show pfe tcam app lfm-802.3ah-in list-shared-apps
show pfe tcam app lfm-802.3ah-in shared-usage
detail
show pfe tcam app lfm-802.3ah-out
<get-pfe-tcam-app-list-lfm-802.3ah-out>
show pfe tcam app lfm-802.3ah-out detail
show pfe tcam app lfm-802.3ah-out list-related-apps
show pfe tcam app lfm-802.3ah-out list-shared-apps
show pfe tcam app lfm-802.3ah-out shared-usage
detail
show pfe tcam app lo0-inet-fil
<get-pfe-tcam-app-list-lo0-inet-fil>
show pfe tcam app lo0-inet-fil detail
show pfe tcam app lo0-inet-fil list-related-apps
show pfe tcam app lo0-inet-fil list-shared-apps
show pfe tcam app lo0-inet-fil shared-usage
detail
show pfe tcam app lo0-inet-fil
<get-pfe-tcam-app-list-lo0-inet6-fil>
show pfe tcam app lo0-inet6-fil detail
show pfe tcam app lo0-inet6-fil list-related-apps
show pfe tcam app lo0-inet6-fil list-shared-apps
show pfe tcam app lo0-inet6-fil shared-usage
detail
show pfe tcam app lo0-inet6-fil
<get-pfe-tcam-app-list-mac-drop-cnt>
show pfe tcam app mac-drop-cnt detail
show pfe tcam app mac-drop-cnt list-related-apps
show pfe tcam app mac-drop-cnt list-shared-apps
show pfe tcam app mac-drop-cnt shared-usage
detail
show pfe tcam app mrouter-port-in
<get-pfe-tcam-app-list-mrouter-port-in>
show pfe tcam app mrouter-port-in detail
show pfe tcam app mrouter-port-in list-related-apps
show pfe tcam app mrouter-port-in list-shared-apps
show pfe tcam app mrouter-port-in shared-usage
detail
show pfe tcam app mrouter-port-in
<get-pfe-tcam-app-list-napt-reverse-fil>
show pfe tcam app napt-reverse-fil detail
show pfe tcam app napt-reverse-fil list-related-apps
show pfe tcam app napt-reverse-fil list-shared-apps
show pfe tcam app napt-reverse-fil shared-usage
detail
show pfe tcam app napt-reverse-fil
<get-pfe-tcam-app-list-no-local-switching>
show pfe tcam app no-local-switching
show pfe tcam app no-local-switching detail
show pfe tcam app no-local-switching list-related-apps
show pfe tcam app no-local-switching list-shared-apps
show pfe tcam app no-local-switching shared-usage
show pfe tcam app no-local-switching shared-usage detail
show pfe tcam app ptpoe-cos-rw
<get-pfe-tcam-app-list-ptpoe-cos-rw>
show pfe tcam app ptpoe-cos-rw detail
show pfe tcam app ptpoe-cos-rw list-related-apps
show pfe tcam app ptpoe-cos-rw list-shared-apps
show pfe tcam app ptpoe-cos-rw shared-usage
show pfe tcam app ptpoe-cos-rw shared-usage detail
show pfe tcam app rfc2544-layer2-in
<get-pfe-tcam-app-list-rfc2544-layer2-in>
  show pfe tcam app rfc2544-layer2-in detail
  show pfe tcam app rfc2544-layer2-in list-related-apps
  show pfe tcam app rfc2544-layer2-in list-shared-apps
  show pfe tcam app rfc2544-layer2-in shared-usage
  show pfe tcam app rfc2544-layer2-in shared-usage detail
show pfe tcam app rfc2544-layer2-out
<get-pfe-tcam-app-list-rfc2544-layer2-out>
show pfe tcam app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam app vpls-mesh-group-mcast detail
show pfe tcam app vpls-mesh-group-mcast list-related-apps
show pfe tcam app vpls-mesh-group-mcast list-shared-apps
show pfe tcam app vpls-mesh-group-mcast shared-usage
details
show pfe tcam app vpls-mesh-group-mcast shared-usage detail
show pfe tcam app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam app vpls-mesh-group-ucast detail
show pfe tcam app vpls-mesh-group-ucast list-related-apps
show pfe tcam app vpls-mesh-group-ucast list-shared-apps
show pfe tcam app vpls-mesh-group-ucast shared-usage
details
show pfe tcam app cfm-filter detail
show pfe tcam errors app fw-inet-rpf
<get-pfe-tcam-errors-app-fw-inet-rpf>
show pfe tcam errors app fw-inet-rpf detail
show pfe tcam errors app fw-inet-rpf list-related-apps
show pfe tcam errors app fw-inet-rpf list-shared-apps
show pfe tcam errors app fw-inet-rpf shared-usage
show pfe tcam errors app vpls-mesh-group-mcast shared-usage detail
show pfe tcam errors app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam errors app vpls-mesh-group-ucast detail
show pfe tcam errors app vpls-mesh-group-ucast list-related-apps
show pfe tcam errors app vpls-mesh-group-ucast list-shared-apps
show pfe tcam errors app vpls-mesh-group-ucast shared-usage
show pfe tcam errors app vpls-mesh-group-ucast shared-usage detail
show pfe tcam errors tcam-stage ingress app fw-inet-rpf
<get-pfe-tcam-errors-ingress-tcam-stage-fw-inet-rpf>
show pfe tcam errors tcam-stage ingress app fw-inet-rpf detail
show pfe tcam errors tcam-stage ingress app fw-inet-rpf list-related-apps
show pfe tcam errors tcam-stage ingress app fw-inet-rpf list-shared-apps
show pfe tcam errors tcam-stage ingress app fw-inet-rpf shared-usage
show pfe tcam errors tcam-stage ingress app fw-inet-rpf shared-usage detail
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf
<get-pfe-tcam-errors-ingress-tcam-stage-fw-inet6-rpf>
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf detail
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf list-related-apps
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf list-shared-apps
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf shared-usage
show pfe tcam errors tcam-stage ingress app fw-inet6-rpf shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-egr>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr shared-usage
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-egr shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-ing>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing shared-usage
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-ing shared-usage detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing
<get-pfe-tcam-errors-ingress-tcam-stage-gr-ifl-statistics-preing>
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing detail
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing
list-related-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing
list-shared-apps
show pfe tcam errors tcam-stage ingress app gr-ifl-stats-preing shared-usage
detail
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff
<get-pfe-tcam-errors-pre-ingress-app-ing-out-iff>
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff detail
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff list-related-apps
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app ing-out-iff shared-usage
detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-related-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-mcast shared-usage
detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast detail
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-related-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast list-shared-apps
show pfe tcam errors tcam-stage pre-ingress app vpls-mesh-group-ucast shared-usage
detail
show pfe tcam usage app fw-inet-rpf
<get-pfe-tcam-usage-app-fw-inet-rpf>
show pfe tcam usage app fw-inet-rpf detail
show pfe tcam usage app fw-inet-rpf list-related-apps
show pfe tcam usage app fw-inet-rpf list-shared-apps
show pfe tcam usage app fw-inet-rpf shared-usage
show pfe tcam usage app fw-inet-rpf shared-usage detail
show pfe tcam usage app fw-inet6-rpf
<get-pfe-tcam-usage-app-fw-inet6-rpf>
show pfe tcam usage app fw-inet6-rpf detail
show pfe tcam usage app fw-inet6-rpf list-related-apps
show pfe tcam usage app fw-inet6-rpf list-shared-apps
show pfe tcam usage app fw-inet6-rpf shared-usage
show pfe tcam usage app fw-inet6-rpf shared-usage detail
show pfe tcam usage app gr-ifl-stats-egr
<get-pfe-tcam-usage-app-gr-ifl-statistics-egr>
show pfe tcam usage app gr-ifl-stats-egr detail
show pfe tcam usage app gr-ifl-stats-egr list-related-apps
show pfe tcam usage app gr-ifl-stats-egr list-shared-apps
show pfe tcam usage app gr-ifl-stats-egr shared-usage
show pfe tcam usage app gr-ifl-stats-egr shared-usage detail
show pfe tcam usage app gr-ifl-stats-ing
<get-pfe-tcam-usage-app-gr-ifl-statistics-ing>
show pfe tcam usage app gr-ifl-stats-ing detail
show pfe tcam usage app gr-ifl-stats-ing list-related-apps
show pfe tcam usage app gr-ifl-stats-ing list-shared-apps
show pfe tcam usage app gr-ifl-stats-ing shared-usage
show pfe tcam usage app gr-ifl-stats-ing shared-usage detail
show pfe tcam usage app gr-ifl-stats-preing
<get-pfe-tcam-usage-app-gr-ifl-statistics-preing>
show pfe tcam usage app gr-ifl-stats-preing detail
show pfe tcam usage app gr-ifl-stats-preing list-related-apps
show pfe tcam usage app gr-ifl-stats-preing list-shared-apps
show pfe tcam usage app gr-ifl-stats-preing shared-usage
show pfe tcam usage app gr-ifl-stats-preing shared-usage detail
show pfe tcam usage app ing-out-iff
<get-pfe-tcam-usage-app-ing-out-iff>
show pfe tcam usage app ing-out-iff detail
show pfe tcam usage app ing-out-iff list-related-apps
show pfe tcam usage app ing-out-iff list-shared-apps
show pfe tcam usage app ing-out-iff shared-usage
show pfe tcam usage app ing-out-iff shared-usage detail
show pfe tcam usage app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam usage app vpls-mesh-group-mcast detail
show pfe tcam usage app vpls-mesh-group-mcast list-related-apps
show pfe tcam usage app vpls-mesh-group-mcast list-shared-apps
show pfe tcam usage app vpls-mesh-group-mcast shared-usage
show pfe tcam usage app vpls-mesh-group-mcast shared-usage detail
show pfe tcam usage app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam usage app vpls-mesh-group-ucast detail
show pfe tcam usage app vpls-mesh-group-ucast list-related-apps
show pfe tcam usage app vpls-mesh-group-ucast list-shared-apps
show pfe tcam usage app vpls-mesh-group-ucast shared-usage
detail
show pfe tcam usage tcam-stage egress app rfc2544-layer2-out shared-usage
detail
get-pfe-tcam-usage-egress-tcam-stage-detail
show pfe tcam usage tcam-stage ingress
<get-pfe-tcam-usage-ingress-tcam-stage>
show pfe tcam usage tcam-stage ingress app
cfm-bd-filter
<get-pfe-tcam-usage-ingress-app-cfm-bd-filter>
show pfe tcam usage tcam-stage ingress app cfm-bd-filter
detail
show pfe tcam usage tcam-stage ingress app cfm-bd-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-bd-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-bd-filter shared-usage
detail
show pfe tcam usage tcam-stage ingress app cfm-filter
<get-pfe-tcam-usage-ingress-app-cfm-filter>
show pfe tcam usage tcam-stage ingress app cfm-filter detail
show pfe tcam usage tcam-stage ingress app cfm-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-filter shared-usage
detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter
<get-pfe-tcam-usage-ingress-app-cfm-vpls-filter>
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-filter shared-usage
detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter
<get-pfe-tcam-usage-ingress-app-cfm-vpls-ifl-filter>
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter detail
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter
list-related-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter list-shared-apps
show pfe tcam usage tcam-stage ingress app cfm-vpls-ifl-filter shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-ccc-in
<get-pfe-tcam-usage-ingress-app-fw-ccc-in>
show pfe tcam usage tcam-stage ingress app fw-ccc-in detail
show pfe tcam usage tcam-stage ingress app fw-ccc-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-ccc-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-ccc-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-ifl-in
<get-pfe-tcam-usage-ingress-app-fw-ifl-in>
show pfe tcam usage tcam-stage ingress app fw-ifl-in detail
show pfe tcam usage tcam-stage ingress app fw-ifl-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-ifl-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-ifl-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet-ftf
<get-pfe-tcam-usage-ingress-app-fw-inet-ftf>
show pfe tcam usage tcam-stage ingress app fw-inet-ftf detail
show pfe tcam usage tcam-stage ingress app fw-inet-ftf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-ftf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-ftf shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet-in
<get-pfe-tcam-usage-ingress-app-fw-inet-in>
show pfe tcam usage tcam-stage ingress app fw-inet-in detail
show pfe tcam usage tcam-stage ingress app fw-inet-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet-pm
<get-pfe-tcam-usage-ingress-app-fw-inet-pm>
show pfe tcam usage tcam-stage ingress app fw-inet-pm detail
show pfe tcam usage tcam-stage ingress app fw-inet-pm list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-pm list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-pm shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet-rpf
<get-pfe-tcam-usage-ingress-app-fw-inet-rpf>
show pfe tcam usage tcam-stage ingress app fw-inet-rpf detail
show pfe tcam usage tcam-stage ingress app fw-inet-rpf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet-rpf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet-rpf shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf
<get-pfe-tcam-usage-ingress-app-fw-inet6-ftf>
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf detail
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-ftf shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet6-in
<get-pfe-tcam-usage-ingress-app-fw-inet6-in>
show pfe tcam usage tcam-stage ingress app fw-inet6-in detail
show pfe tcam usage tcam-stage ingress app fw-inet6-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf
<get-pfe-tcam-usage-ingress-app-fw-inet6-rpf>
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf detail
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf list-related-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-inet6-rpf shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-l2-in
<get-pfe-tcam-usage-ingress-app-fw-l2-in>
show pfe tcam usage tcam-stage ingress app fw-l2-in detail
show pfe tcam usage tcam-stage ingress app fw-l2-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-l2-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-l2-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-mpls-in
<get-pfe-tcam-usage-ingress-app-fw-mpls-in>
show pfe tcam usage tcam-stage ingress app fw-mpls-in detail
show pfe tcam usage tcam-stage ingress app fw-mpls-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-mpls-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-mpls-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app fw-vpls-in
<get-pfe-tcam-usage-ingress-app-fw-vpls-in>
show pfe tcam usage tcam-stage ingress app fw-vpls-in detail
show pfe tcam usage tcam-stage ingress app fw-vpls-in list-related-apps
show pfe tcam usage tcam-stage ingress app fw-vpls-in list-shared-apps
show pfe tcam usage tcam-stage ingress app fw-vpls-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-egr>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-egr shared-usage
detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-ing>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-ing shared-usage
detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing
<get-pfe-tcam-usage-ingress-app-gr-ifl-statistics-preing>
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing detail
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing list-related-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing list-shared-apps
show pfe tcam usage tcam-stage ingress app gr-ifl-stats-preing shared-usage
detail
show pfe tcam usage tcam-stage ingress app ifl-statistics-in
<get-pfe-tcam-usage-ingress-app-ifl-statistics-in>
show pfe tcam usage tcam-stage ingress app ifl-statistics-in detail
show pfe tcam usage tcam-stage ingress app ifl-statistics-in list-related-apps
show pfe tcam usage tcam-stage ingress app ifl-statistics-in list-shared-apps
show pfe tcam usage tcam-stage ingress app ifl-statistics-in shared-usage
detail
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil
<get-pfe-tcam-usage-ingress-app-ipsec-reverse-fil>
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil detail
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil list-related-apps
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app ipsec-reverse-fil shared-usage
detail
show pfe tcam usage tcam-stage ingress app irb-fixed-cos
<get-pfe-tcam-usage-ingress-app-irb-fixed-cos>
detail
list-related-apps
list-shared-apps
shared-usage
shared-usage detail
<get-pfe-tcam-usage-ingress-app-irb-inet6-fil>
detail
list-related-apps
list-shared-apps
shared-usage
shared-usage detail
<get-pfe-tcam-usage-ingress-app-lfm-802.3ah-in>
detail
list-related-apps
list-shared-apps
shared-usage
shared-usage detail
<get-pfe-tcam-usage-ingress-app-lo0-inet-fil>
detail
list-related-apps
list-shared-apps
shared-usage
shared-usage detail
<get-pfe-tcam-usage-ingress-app-lo0-inet6-fil>
detail
list-related-apps
list-shared-apps
shared-usage
shared-usage detail
<get-pfe-tcam-usage-ingress-app-mac-drop-cnt>
detail
show pfe tcam usage tcam-stage ingress app mac-drop-cnt list-related-apps
show pfe tcam usage tcam-stage ingress app mac-drop-cnt list-shared-apps
show pfe tcam usage tcam-stage ingress app mac-drop-cnt shared-usage
detail
<get-pfe-tcam-usage-ingress-app-mrouter-port-in>
show pfe tcam usage tcam-stage ingress app mrouter-port-in list-related-apps
show pfe tcam usage tcam-stage ingress app mrouter-port-in list-shared-apps
show pfe tcam usage tcam-stage ingress app mrouter-port-in shared-usage
detail
<get-pfe-tcam-usage-ingress-app-napt-reverse-fil>
show pfe tcam usage tcam-stage ingress app napt-reverse-fil list-related-apps
show pfe tcam usage tcam-stage ingress app napt-reverse-fil list-shared-apps
show pfe tcam usage tcam-stage ingress app napt-reverse-fil shared-usage
detail
<get-pfe-tcam-usage-ingress-app-no-local-switching>
show pfe tcam usage tcam-stage ingress app no-local-switching list-related-apps
show pfe tcam usage tcam-stage ingress app no-local-switching list-shared-apps
show pfe tcam usage tcam-stage ingress app no-local-switching shared-usage
detail
<get-pfe-tcam-usage-ingress-tcam-stage-detail>
show pfe tcam usage tcam-stage pre-ingress list-related-apps
show pfe tcam usage tcam-stage pre-ingress list-shared-apps
show pfe tcam usage tcam-stage pre-ingress shared-usage
detail
<get-pfe-tcam-usage-pre-ingress-tcam-stage>
show pfe tcam usage tcam-stage pre-ingress app cos-fc list-related-apps
show pfe tcam usage tcam-stage pre-ingress app cos-fc list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app cos-fc shared-usage
detail
<get-pfe-tcam-usage-pre-ingress-app-fw-fbf>
show pfe tcam usage tcam-stage pre-ingress app fw-fbf detail
<get-pfe-tcam-usage-pre-ingress-app-ip-mac-val-bcast>
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast detail
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast
list-related-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app ip-mac-val-bcast shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in
<get-pfe-tcam-usage-pre-ingress-app-rfc2544-layer2-in>
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in detail
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in
list-related-apps
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app rfc2544-layer2-in shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast
<get-upper-level-xml-name-vpls-mesh-group-mcast>
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast
list-related-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-mcast
shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
<get-upper-level-xml-name-vpls-mesh-group-ucast>
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-related-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
shared-usage
detail
show pfe tcam usage tcam-stage pre-ingress app vpls-mesh-group-ucast
list-shared-apps
<get-pfe-tcam-usage-pre-ingress-tcam-stage-detail>
show pfe terse
   <get-pfe-information>

show pfe version brief
show pfe version detail
show pgm
show pgm negative-acknowledgments
   <get-pgm-nak>

show pgm source-path-messages
   <get-pgm-source-path-messages>

show pgm statistics
   <get-pgm-statistics>

show pim
show pim bidirectional
show pim bidirectional df-election
   <get-pim-bidir-df-election-information>
show pim bidirectional df-election interface
   <get-pim-bidir-df-election-interface-information>
show pim bootstrap
   <get-pim-bootstrap-information>

show pim interfaces
   <get-pim-interfaces-information>

show pim join
   <get-pim-join-information>

show pim mdt
   <get-pim-mdt-information>

show pim mdt data-mdt-joins
   <get-pim-data-mdt-join-information>
show pim mvnp
   <get-pim-mvnp-information>

show pim neighbors
   <get-pim-neighbors-information>
show pim rps
    <get-pim-rps-information>
show pim snooping
show pim snooping interfaces
show pim snooping join
show pim snooping neighbors
show pim snooping statistics
show pim source
    <get-pim-source-information>

show pim statistics
    <get-pim-statistics-information>

show policy
show policy conditions
show policy damping
show ppp
show ppp address-pool
    <get-ppp-address-pool-information>

show ppp interface
    <get-ppp-interface-information>

show ppp statistics
    <get-ppp-statistics-information>

show ppp summary
    <get-ppp-summary-information>

show pppoe
show pppoe interfaces
    <get-pppoe-interface-information>
show pppoe lockout
    <get-pppoe-lockout-information>
show pppoe lockout atm-identifier
    <get-pppoe-lockout-atm-information>
show pppoe lockout vlan-identifier
    <get-pppoe-lockout-vlan-information>

show pppoe service-name-tables
    <get-pppoe-service-name-table-information>
show pppoe statistics
    <get-pppoe-statistics-information>

show pppoe underlying-interfaces
    <get-pppoe-underlying-interface-information>

show pppoe version
    <get-pppoe-version>
show programmable-rpd
show programmable-rpd clients
    <get-programmable-rpd-client-information>

show protection-group
show protection-group ethernet-aps
    <show-protection-group-ethernet-aps>
show protection-group ethernet-ring
show protection-group ethernet-ring aps
    <get-raps-pdu-information>
show protection-group ethernet-ring data-channel
    <get-ring-data-channel-information>
show protection-group ethernet-ring interface
    <get-ring-interface-information>
show protection-group ethernet-ring node-state
    <get-raps-state-machine-information>
show protection-group ethernet-ring node-state
show protection-group ethernet-ring statistics
    <get-ring-statistics>
show protection-group ethernet-ring vlan
    <get-ring-vlan-information>
show ptp
show ptp clock
    <get-tp-clock>
show ptp global-information
    <get-tpg-global-information>
show ptp hybrid
show ptp hybrid config
    <get-tp-hybrid-mapping>
show ptp hybrid status
    <get-tp-hybrid-status>
show ptp last-tod-update
    <get-last-tod-update>
show ptp lock-status
get-ptp-lock-status>
 show ptp master
 <get-ptp-master>
 show ptp path-trace
 <get-ptp-path-trace>
 show ptp port
 <get-ptp-port>
 show ptp quality-level-mapping
 <get-ptp-quality-level-mapping>
 show ptp slave
 <get-ptp-slave>
 show ptp stateful
 <get-ptp-stateful>
 show ptp statistics
 <get-ptp-statistics>
 show r2cp
 show r2cp interfaces
 <get-r2cp-interface-information>
 show r2cp radio
 <get-r2cp-radio-information>
 show r2cp sessions
 <get-r2cp-session-information>
 show r2cp statistics
 <get-r2cp-statistics>
 show redundant-power-system
 show redundant-power-system led
 show redundant-power-system multi-backup
 <get-rps-scale-information>
 show redundant-power-system network
 <get-rps-network-information>
 show redundant-power-system power-supply
 show redundant-power-system status
 show redundant-power-system upgrade
 <get-rps-upgrade-information>
 show redundant-power-system version
 show rip
 show rip general-statistics
 <get-rip-general-statistics-information>

 show rip neighbor
 <get-rip-neighbor-information>
show rip statistics
    <get-rip-statistics-information>
show rip statistics peer
    <get-rip-peer-information>
show ripng
    show ripng general-statistics
        <get-ripng-general-statistics-information>
show ripng neighbor
    <get-ripng-neighbor-information>
show ripng statistics
    <get-ripng-statistics-information>
show route
    <get-route-information>
show route cumulative
    <get-route-cumulative>
show route export
    <get-rteexport-table-information>
show route export instance
    <get-rteexport-instance-information>
show route localization
    <get-fib-localization-information>
show route export vrf-target
    <get-rteexport-target-information>
show route flow
show route flow validation
    <get-rtflow-dep-information>
show route forwarding-table
    <get-forwarding-table-information>
show route instance
    <get-instance-information>
show route instance operational
    <get-operational-routing-instance-information>
show route martians
<get-route-martians>
show route resolution
<get-route-resolution-information>
show route resolution summary
<get-route-resolution-summary>
show route resolution unresolved
show route rib-groups
<get-route-rib-groups>
show route snooping
<get-route-snooping-information>
show route snooping summary
<get-route-snooping-summary>
show route summary
<get-route-summary-information>

show rsvp
show rsvp interface
<get-rsvp-interface-information>

show rsvp neighbor
<get-rsvp-neighbor-information>

show rsvp route-session-id
<get-rsvp-route-session-id-information>

show rsvp session
<get-rsvp-session-information>

show rsvp statistics
<get-rsvp-statistics-information>

show rsvp version
<get-rsvp-version-information>

show sap
show sap listen
<get-sap-listen-information>
show security group-vpn member kek
show security group-vpn member kek security-associations
<get-gvpn-kek-security-associations-information>
show services
show services accounting
  <get-service-accounting-information>

show services accounting aggregation
  <get-service-accounting-aggregation-information>

show services accounting aggregation as
  <get-service-accounting-aggregation-as-information>

show services accounting aggregation destination-prefix
  <get-service-accounting-aggregation-destination-prefix-information>

show services accounting aggregation protocol-port
  <get-service-accounting-aggregation-protocol-port-information>

show services accounting aggregation source-destination-prefix
  <get-service-accounting-aggregation-source-destination-prefix-information>

show services accounting aggregation source-prefix
  <get-service-accounting-aggregation-source-prefix-information>

show services accounting aggregation template
  <get-service-accounting-aggregation-template-information>

show services accounting errors
  <get-service-accounting-errors-information>

show services accounting flow
  <get-service-accounting-flow-information>

show services accounting flow-detail
  <get-service-accounting-flow-detail>

show services accounting memory
  <get-service-accounting-memory-information>

show services accounting packet-size-distribution
  <get-packet-distribution-information>

show services accounting status
  <get-service-accounting-status-information>
show services accounting usage
  <get-service-accounting-usage-information>

show services alg
show services alg conversations
  <get-service-msp-alg-conversation-information>
show services alg sip-globals
<get-service-msp-alg-sip-globals-information>
show services alg statistics
show services application-aware-access-list
show services application-aware-access-list flows
show services application-aware-access-list flows interface
  <get-application-aware-access-list-flows-interface>
show services application-aware-access-list flows subscriber
  <get-application-aware-access-list-flows-subscriber>
show services application-aware-access-list statistics
show services application-aware-access-list statistics interface
  <get-application-aware-access-list-statistics-interface>
show services application-aware-access-list statistics subscriber
  <get-application-aware-access-list-statistics-subscriber>
show services application-identification
show services application-identification application
show services application-identification application detail
  <get-appid-application-signature-detail>
show services application-identification application summary
  <get-appid-application-signature-summary>
show services application-identification application-system-cache
  <get-appid-application-system-cache>

show services application-identification counter
  <get-appid-counter>
show services application-identification counter ssl-encrypted-sessions
<get-appid-counter-encrypted>
show services application-identification group
show services application-identification group detail
  <get-appid-application-group-detail>
show services application-identification group summary
  <get-appid-application-group-summary>
show services application-identification statistics
show services application-identification statistics application-groups
show services border-signaling-gateway embedded-spdf
    <get-service-border-signaling-gateway-embedded-spdf>

show services border-signaling-gateway embedded-spdf status
    <get-service-border-signaling-gateway-embedded-spdf-status>

show services border-signaling-gateway name-resolution-cache

show services border-signaling-gateway name-resolution-cache all
    <get-service-border-signaling-gateway-name-resolution-cache-all>

show services border-signaling-gateway name-resolution-cache by-fqdn
    <get-border-signaling-gateway-name-resolution-cache-by-fqdn>

show services border-signaling-gateway status
    <get-service-bsg-status-information>

show services captive-portal-content-delivery

show services captive-portal-content-delivery pic
    <get-cpcd-pic-information>

show services captive-portal-content-delivery profile
    <get-cpcd-profile>

show services captive-portal-content-delivery rule
    <get-cpcd-rule>

show services captive-portal-content-delivery ruleset
    <get-cpcd-rule-set>

show services captive-portal-content-delivery sset
    <get-cpcd-service-set>

show services captive-portal-content-delivery statistics
    <get-cpcd-pic-statistics>

show services captive-portal-content-delivery statistics interface

show services captive
    <get-service-capture>

show services cos

show services cos statistics
    <get-service-cos-statistics-information>

show services cos statistics diffserv
    <get-service-cos-diffserv-statistics>

show services cos statistics forwarding-class
    <get-service-cos-forwarding-class-statistics>
show services crtp
  <get-service-crtp-params-information>

show services crtp extensive
  <get-service-crtp-extensive-information>

show services crtp flows
  <get-service-crtp-flow-table-information>

show services dynamic-flow-capture
show services dynamic-flow-capture content-destination
  <get-services-dynamic-flow-capture-content-destination-information>

show services dynamic-flow-capture control-source
  <get-services-dynamic-flow-capture-control-source-information>

show services dynamic-flow-capture statistics
  <get-services-dfc-statistics-information>
show extension-service
show extension-service status
  <jet-application-status>
show services fips
show system commit synchronize-server pending-jobs
  <get-pending-commit-sync-jobs>
show services fips pic
show services fips pic status
  <get-fips-pic-status-information>

show services flow-collector
  <get-services-flow-collector-information>

show services flow-collector file
  <get-services-flow-collector-file-information>

show services flow-collector input
  <get-services-flow-collector-input-information>

show services flow-table
show services flow-table statistics
  <get-flow-table-statistics-information>

show services flows
<get-service-msp-flow-table-information>

show services ggsn
show services ggsn diagnostics
show services ggsn diagnostics pdp
  <get-pdp-diagnostics-per-apn>

show services ggsn statistics
  <get-ggsn-statistics>

show services ggsn statistics apn
  <get-ggsn-apn-statistics-information>

show services ggsn statistics charging
  <get-ggsn-charging-statistics-information>

show services ggsn statistics gtp
  <get-ggsn-gtp-statistics-information>

show services ggsn statistics gtp-prime
  <get-ggsn-gtp-prime-statistics-information>

show services ggsn statistics imsi
  <get-ggsn-imsi-user-information>

show services ggsn statistics l2tp-tunnel
  <get-ggsn-l2tp-tunnel-statistics-information>

show services ggsn statistics msisdn
show services ggsn statistics radius
  <get-ggsn-radius-statistics-information>

show services ggsn statistics sgsn
  <get-ggsn-sgsn-statistics-information>

show services ggsn status
  <get-ggsn-interface-information>

show services ggsn trace
show services ggsn trace all
  <get-ggsn-trace>
show services ggsn trace imsi
   <get-ggsn-imsi-trace>

show services ggsn trace msisdn
   <get-ggsn-msisdn-trace>
show services ha
   <get-service-ha-info>
show services hcm
   <get-service-hcm-pic-statistics-information>
show services ids
   <get-service-ids-destination-table-information>
   <get-service-ids-pair-table-information>
   <get-service-ids-source-table-information>
show services inline
   <get-inline-nat-mapping-nptv6-information>
show services inline ip-reassembly
show services inline ip-reassembly statistics
show services inline nat
   <get-inline-nat-pool-information>
   <get-inline-nat-statistics-information>
show services inline nat mappings
show services inline nat mappings nptv6
show services inline softwire
   <get-inline-service-sw-statistics-information>
show services inline stateful-firewall
show services inline stateful-firewall flows
show services inline stateful-firewall statistics
show services ipsec-vpn
   <get-inline-sfw-flow-table-information>
show services ipsec-vpn ike
show services ipsec-vpn ike security-associations
<get-ike-services-security-associations-information>

show services ipsec-vpn ike statistics
<get-ike-services-statistics>
show services ipsec-vpn ipsec
show services ipsec-vpn ipsec security-associations
<get-services-security-associations-information>

show services ipsec-vpn ipsec statistics
<get-services-ipsec-statistics-information>

show services l2tp
show services l2tp client
<get-l2tp-client-information>
show services l2tp destination
<get-l2tp-destination-information>
show services l2tp destination lockout
<get-services-l2tp-destination-lockout>
show services l2tp disconnect-cause-summary
<get-l2tp-disconnect-cause-summary>
show services l2tp multilink
<get-l2tp-multilink-information>

show services l2tp radius
show services l2tp radius accounting
show services l2tp radius accounting servers
<get-services-l2tp-radius-accounting-servers-information>

show services l2tp radius accounting statistics
<get-services-l2tp-radius-accounting-statistics-information>

show services l2tp radius authentication
show services l2tp radius authentication servers
<get-services-l2tp-radius-authentication-servers-information>

show services l2tp radius authentication statistics
<get-services-l2tp-radius-authentication-statistics-information>

show services l2tp radius servers
<get-services-l2tp-radius-authentication-accounting-servers-information>

show services l2tp radius statistics
show services l2tp session
<get-l2tp-session-information>
show services l2tp session-limit-group
<get-l2tp-session-limit-group-information>

show services l2tp summary
<get-l2tp-summary-information>

show services l2tp tunnel
<get-l2tp-tunnel-information>
show services l2tp tunnel-group
<get-l2tp-tunnel-group-information>

show services l2tp user
<get-l2tp-user-information>
show services link-services
show services link-services cpu-usage
<get-link-services-cpu-usage>

show services local-policy-decision-function
show services local-policy-decision-function flows
show services local-policy-decision-function flows interface
<get-local-policy-decision-function-flows-interface>
show services local-policy-decision-function flows subscriber
<get-local-policy-decision-function-flows-subscriber>
show services local-policy-decision-function statistics
show services local-policy-decision-function statistics interface
<get-local-policy-decision-function-statistics-interface>
show services local-policy-decision-function statistics subscriber
<get-local-policy-decision-function-statistics-subscriber>

show services logging
show services logging history
show services logging history client
show services logging logfiles
show services match-policies
<get-services-match-policies>
show services mobile
show services mobile hcm
show services mobile hcm statistics
show services nat
show services nat ipv6-multicast-interfaces
   <get-service-nat-ipv6-multicast-information>

show services nat deterministic-nat
show services nat deterministic-nat internal-host
show services nat deterministic-nat nat-port-block
show services nat mappings
   <get-service-nat-mapping-address-pooling-paired>
show services nat mappings brief
<get-service-nat-mapping-brief>
show services nat mappings detail
show services nat mappings endpoint-independent
   <get-service-nat-mapping-endpoint-independent>
show services nat mappings brief
   <get-service-nat-mapping-brief>
show services nat mappings detail
   <get-service-nat-mapping-detail>
show services nat mappings pcp
show services nat mappings summary
   <get-service-nat-mapping-summary>
show services nat pool
   <get-service-nat-pool-information>
show services pcp
show services pgcp
show services pgcp active-configuration
   <get-pgcpd-active-configuration>

show services pgcp active-configuration gateway
   <get-service-pgcp-active-configuration-gateway>

show services pgcp conversations
   <get-service-pgcp-conversation-information>

show services pgcp conversations gateway
   <get-service-pgcp-conversation-information-gateway>

show services pgcp flows
   <get-service-pgcp-flow-table-information>

show services pgcp flows gateway
   <get-service-pgcp-flow-table-information-gateway>
show services pgcp gate
   <get-service-pgcp-gate>

show services pgcp gate gateway
   <get-service-pgcp-gate-gateway>

show services pgcp gates
   <get-service-pgcp-gates>

show services pgcp gates gateway
   <get-service-pgcp-gates-gateway>

show services pgcp root-termination
   <get-services-pgcpd-root-termination>

show services pgcp root-termination gateway
   <get-services-pgcpd-root-termination-gateway>

show services pgcp statistics
   <get-service-pgcp-statistics>

show services pgcp statistics gateway
   <get-service-pgcp-statistics-gateway>

show services pgcp terminations
   <get-service-pgcp-terminations>

show services pgcp terminations gateway
   <get-service-pgcp-terminations-gateway>

show services redundancy-group
   <get-services-redundancy-group-information>
show services redundancy-group rg-id
   <get-services-redundancy-group-id-information>

show services rpm
show services rpm active-servers
   <get-active-servers>

show services rpm history-results
   <get-history-results>

show services rpm probe-results
<get-probe-results>

show services rpm twamp
  <twamp-information>
show services rpm twamp client
  <twamp-client-information>
show services rpm twamp client connection
  <twamp-client-connection-information>
show services rpm twamp client history-results
  <twamp-get-history-results>
show services rpm twamp client probe-results
  <twamp-get-probe-results>
show services rpm twamp client session
  <twamp-client-test-session>
show services rpm twamp server
  <twamp-server-information>
show services rpm twamp server connection
  <twamp-server-connection-information>
show services rpm twamp server session
  <twamp-server-session-information>
show services server-load-balance
show services server-load-balance external-manager
show services server-load-balance external-manager information
show services server-load-balance external-manager statistics
  <get-external-manager-statistics-information>
show services server-load-balance hash-table
  <get-hash-table-information>
show services server-load-balance health-monitor
show services server-load-balance health-monitor information
  <get-real-server-health-monitor-information>
show services server-load-balance health-monitor statistics
  <get-real-server-health-monitor-statistics-information>
show services server-load-balance real-server
show services server-load-balance real-server statistics
  <get-real-server-statistics-information>
show services server-load-balance real-server-group
show services server-load-balance real-server-group information
  <get-real-server-group-information>
show services server-load-balance real-server-group statistics
  <get-real-server-group-statistics-information>
show services server-load-balance sticky
  <get-sticky-table-information>
show services server-load-balance virtual-server
show services server-load-balance virtual-server information
   <get-virtual-server-information>
show services server-load-balance virtual-server statistics
   <get-virtual-server-statistics-information>
show services service-identification
show services service-identification header-redirect
show services service-identification header-redirect statistics
   <get-header-redirect-set-statistics-information>
show services service-identification statistics
   <get-service-identification-statistics-information>
show services service-identification uri-redirect
show services service-identification uri-redirect statistics
   <get-uri-redirect-set-statistics-information>
show services service-sets
show services service-sets cpu-usage
   <get-service-set-cpu-statistics>
show services service-sets memory-usage
   <get-service-set-memory-statistics>
show services service-sets memory-usage zone
show services service-sets plug-ins
   <get-service-set-plugin-summary>
show services service-sets statistics
show services service-sets statistics drop-flow-limit
   <get-service-set-drop-flow-statistics>
show services service-sets statistics ids
show services service-sets statistics ids drops
   <get-service-set-ids-drops-statistics>
show services service-sets statistics jflow-log
   <get-service-set-jflow-log-statistics>
show services service-sets statistics packet-drops
   <get-service-set-packet-drop-statistics>
show services service-sets statistics syslog
   <get-service-set-syslog-statistics>
show services service-sets statistics tcp
<get-service-set-tcp-tracker-statistics>
show services service-sets statistics tcp-mss
  <get-service-set-tcp-mss-statistics>

show services service-sets summary
  <get-service-set-summary-information>

show services sessions
  <get-msp-session-table>
show services sessions analysis
  <show-service-msp-session-analysis-information>
show services sessions count
  <get-service-msp-sess-count-information>
show services sessions utilization
  <get-services-sessions-utilization>

show services softwire
  <get-service-softwire-table-information>

show services softwire flows
  <get-service-fwnat-flow-table-information>

show services softwire statistics
  <get-service-softwire-statistics-information>

show services stateful-firewall
show services stateful-firewall flow-analysis
  <get-service-flow-analysis-information>
show services stateful-firewall conversations
  <get-service-sfw-conversation-information>

show services stateful-firewall flows
  <get-service-sfw-flow-table-information>
show services stateful-firewall redundancy-statistics
  <get-service-sfw-redundancy-statistics>

show services stateful-firewall sip-call
  <get-service-sfw-sip-call-information>

show services stateful-firewall sip-register
  <get-service-sfw-sip-register-information>
show services stateful-firewall statistics
   <get-service-sfw-statistics-information>

show services stateful-firewall statistics application-protocol
<et-sfw-application-protocol-statistics>
show services stateful-firewall subscriber-analysis
<get-service-subs-analysis-information>
show services subscriber
show services subscriber bandwidth
show services subscriber bandwidth client-id
   <get-services-subscriber-bandwidth-by-session-id>
show services subscriber bandwidth interface
   <get-services-subscriber-bandwidth-by-interface>
show services subscriber bandwidth ip-address
   <get-services-subscriber-bandwidth-by-ip-address>
show services subscriber bandwidth service-interface
   <get-services-subscriber-bandwidth-by-service-interface>
show services subscriber dynamic-policies
   <get-services-subscriber-dynamic-policies>
show services subscriber flows
   <get-services-subscriber-flows>
show services subscriber sessions
   <get-services-subscriber-session>
show services subscriber statistics
   <get-services-subscriber-statistics>
show services traffic-detection-function
show services traffic-detection-function hcm
show services traffic-detection-function hcm statistics
<get-service-tdf-hcm-sessions-stats>
show services traffic-detection-function sessions
<get-service-tdf-sessions-information>
show services traffic-load-balance
show services traffic-load-balance statistics
<get-traffic-load-balance-statistics>
show services unified-access-control
show services unified-access-control authentication-table
<get-uac-auth-table>
show services unified-access-control counters
<get-uac-counters>
show services unified-access-control policies
<get-uac-policies>
show services unified-access-control roles
<get-uac-role-entries>
show services unified-access-control status
<get-uac-status>
show services video-monitoring
<get-service-video-monitoring-information>
show services video-monitoring mdi
<get-service-video-monitoring-mdi-information>
show services video-monitoring mdi alarms
<get-services-video-monitoring-mdi-alarms-information>
show services video-monitoring mdi alarms errors
<get-services-video-monitoring-mdi-alarms-errors-information>
show services video-monitoring mdi alarms stats
<get-services-video-monitoring-mdi-alarms-stats-information>
show services video-monitoring mdi errors
<get-service-video-monitoring-mdi-errors-information>
show services video-monitoring mdi flow
<get-service-video-monitoring-mdi-flows-information>
show services video-monitoring mdi stats
<get-service-video-monitoring-mdi-stats-information>
show shmlog
show shmlog argument-mappings
<get-shmlog-argument-mappings>
show shmlog configuration
<show-shmlog-configuration>
show shmlog entries
<show-shmlog-entries>
show shmlog logs-summary
<show-shmlog-logsummary>
show shmlog statistics
<show-shmlog-statistics>
show snmp
show snmp health-monitor
<get-health-monitor-information>
show snmp health-monitor alarms
<get-health-monitor-alarm-information>
show snmp health-monitor logs
<get-health-monitor-log-information>
show snmp health-monitor routing-engine
show snmp health-monitor routing-engine history
<get-health-monitor-routing-engine-history>
show snmp health-monitor routing-engine history cpu
<get-routing-engine-cpu-history>
show snmp health-monitor routing-engine history memory
<get-routing-engine-memory-history>
show snmp health-monitor routing-engine history open-files-count
<get-routing-engine-fd-history>
show snmp health-monitor routing-engine history process-count
<get-routing-engine-pcount-history>
show snmp health-monitor routing-engine history storage
<get-routing-engine-storage-history>
show snmp health-monitor routing-engine history temperature
<get-routing-engine-temperature-history>
show snmp health-monitor routing-engine status
<get-health-monitor-routing-engine-information>
show snmp health-monitor routing-engine status detail

show snmp inform-statistics
  <get-snmp-inform-statistics>

show snmp mib
show snmp mib get
  <get-snmp-object>

show snmp mib get-next
  <get-next-snmp-object>

show snmp mib walk
  <get-walk-snmp-object>

show snmp proxy
show snmp rmon
  <get-rmon-information>

show snmp rmon alarms
  <get-rmon-alarm-information>

show snmp rmon events
  <get-rmon-event-information>

show snmp rmon history
  <get-rmon-history-information>
show snmp rmon logs
  <get-rmon-log-information>

show snmp statistics
  <get-snmp-information>

show snmp v3
  <get-snmp-v3-information>

show snmp v3 access
  <get-snmp-v3-access-information>

show snmp v3 community
  <get-snmp-v3-community-information>

show snmp v3 general
  <get-snmp-v3-general-information>

show snmp v3 groups
  <get-snmp-v3-group-information>

show snmp v3 notify
  <get-snmp-v3-notify-information>

show snmp v3 notify filter
  <get-snmp-v3-notify-filter-information>

show snmp v3 target
  <get-snmp-v3-target-information>

show snmp v3 target address
  <get-snmp-v3-target-address-information>

show snmp v3 target parameters
  <get-snmp-v3-target-parameters-information>

show snmp v3 users
  <get-snmp-v3-usm-user-information>

show spanning-tree
show spanning-tree bridge
<get-stp-bridge-information>
show spanning-tree interface
  <get-stp-interface-information>
show spanning-tree mstp
show spanning-tree mstp configuration
  <get-mstp-configuration-information>
show spanning-tree statistics
  <get-stp-interface-statistics>
show spanning-tree statistics bridge
show spanning-tree statistics interface
show spanning-tree statistics routing-instance
  <get-stp-routing-instance-statistics>
show spanning-tree stp-buffer
show spanning-tree stp-buffer see-all
show ssl-certificates
  <get-ssl-certificate-information>
show static-subscribers
show static-subscribers sessions
  <show subscribers
    <get-subscribers>
show subscribers summary
  <get-subscribers-summary>
<get-syslog-filenames>
show synchronous-ethernet
show synchronous-ethernet esmc
show synchronous-ethernet esmc statistics
show synchronous-ethernet esmc transmit
show synchronous-ethernet global-information
show system
show system alarms
  <get-system-alarm-information>
show system auto-snapshot
show system boot-messages
show system buffers
show system certificate
show system commit
  <get-commit-information>
show system commit revision
<get-commit-revision-information>
show system commit server
show system commit ephemeral
show system commit server queue
show system commit synchronize-server
show system configuration
show system configuration archival
    <get-system-archival>

show system configuration rescue
    <get-rescue-information>

show system connections
show system core-dumps
    <get-system-core-dumps>
show system core-dumps core-file-info
    <get-core-file-information>

show system core-dumps kernel-crashinfo
show system core-dumps satellite
    <get-core-file-satellite>
show system core-dumps transfer-status
show system diagnostics
show system diagnostics inventory
show system diagnostics usage
show system directory-usage
    <get-directory-usage-information>

show system firmware
    <get-system-firmware-information>
show system khms-stats

show system license
    <get-license-summary-information>

show system license installed
    <get-license-information>
show system license key-content
show system license keys
    <get-license-key-information>
show system services dhcp pool
  <get-dhcp-pool-information>

show system services dhcp statistics
  <get-dhcp-statistics-information>

show system services reverse
  <get-system-services-reverse-information>

show system services service-deployment
  <get-service-deployment-service-information>

show system snapshot
  <get-snapshot-information>

show system software
show system software backup
  <get-package-backup-information>
  <get-software-installation-status>
show system software recovery-package
show system software rollback
  <show-package-rollback>

show system statistics
  <get-statistics-information>

show system statistics bridge
  <get-system-bridge-statistics>
show system statistics extended
show system statistics vpls
show system storage
  <get-system-storage>
show system storage partitions
  <get-system-storage-partitions>
show system storage satellite
  <get-system-storage-satellite>
show system subscriber-management
show system subscriber-management arp
  <get-subscriber-management-arp>
show system subscriber-management arp address
  <get-subscriber-management-arp-address>
show system subscriber-management arp interface
<get-subscriber-management-arp-interface>
show system subscriber-management ipv6-neighbors
<get-subscriber-management-ipv6-neighbors>
show system subscriber-management ipv6-neighbors address
<get-subscriber-management-ipv6-neighbor-address>
show system subscriber-management ipv6-neighbors interface
<get-subscriber-management-ipv6-neighbor-interface>
show system subscriber-management route
<get-subscriber-management-route>
show system subscriber-management route next-hop
<get-subscriber-management-route-nh>
show system subscriber-management route prefix
show system subscriber-management route summary
<get-subscriber-management-route-summary>
show system subscriber-management statistics
<get-subscriber-management-statistics>
show system subscriber-management summary
show system switchover
<get-switchover-information>
show system uptime
<get-system-uptime-information>
show system users
<get-system-users-information>
show system virtual-memory
show system yang
show system yang package
<get-system-yang-packages>
show task
show task io
show task logical-system-mux
<get-lrmuxd-task-information>
show task logical-system-mux io
<get-lrmuxd-tasks-io-statistics>
show task logical-system-mux memory
<get-lrmuxd-task-memory>
show task memory
show task replication
<get-routing-task-replication-state>
show task snooping
show task snooping io
show task snooping memory
<get-snooping-task-memory-information>
show ted
show ted database
  <get-ted-database-information>

show ted link
  <get-ted-link-information>

show ted protocol
  <get-ted-protocol-information>
show unified-edge
show unified-edge gateways
show unified-edge ggsn-pgw
show unified-edge ggsn-pgw aaa
show unified-edge ggsn-pgw aaa network-element
show unified-edge ggsn-pgw aaa network-element status
show unified-edge ggsn-pgw aaa network-element-group
show unified-edge ggsn-pgw aaa network-element-group status
show unified-edge ggsn-pgw aaa radius
show unified-edge ggsn-pgw aaa radius statistics
show unified-edge ggsn-pgw aaa statistics
show unified-edge ggsn-pgw address-assignment
show unified-edge ggsn-pgw address-assignment group
show unified-edge ggsn-pgw address-assignment pool
show unified-edge ggsn-pgw address-assignment service-mode
show unified-edge ggsn-pgw address-assignment statistics
show unified-edge ggsn-pgw apn
show unified-edge ggsn-pgw apn service-mode
show unified-edge ggsn-pgw apn statistics
show unified-edge ggsn-pgw call-rate
show unified-edge ggsn-pgw call-rate statistics
show unified-edge ggsn-pgw charging
show unified-edge ggsn-pgw charging global
show unified-edge ggsn-pgw charging global statistics
show unified-edge ggsn-pgw charging local-persistent-storage
show unified-edge ggsn-pgw charging local-persistent-storage statistics
show unified-edge ggsn-pgw charging path
show unified-edge ggsn-pgw charging path statistics
show unified-edge ggsn-pgw charging path status
show unified-edge ggsn-pgw charging service-mode
show unified-edge ggsn-pgw charging transfer
show unified-edge ggsn-pgw charging transfer statistics
show unified-edge ggsn-pgw charging transfer status
show unified-edge ggsn-pgw charging trigger-profile
show unified-edge ggsn-pgw gtp
show unified-edge ggsn-pgw gtp peer
show unified-edge ggsn-pgw gtp peer count
show unified-edge ggsn-pgw gtp peer history
show unified-edge ggsn-pgw gtp peer statistics
show unified-edge ggsn-pgw gtp statistics
show unified-edge ggsn-pgw ip-reassembly
show unified-edge ggsn-pgw ip-reassembly statistics
show unified-edge ggsn-pgw resource-manager
show unified-edge ggsn-pgw resource-manager clients
show unified-edge ggsn-pgw service-mode
show unified-edge ggsn-pgw statistics
show unified-edge ggsn-pgw statistics traffic-class
show unified-edge ggsn-pgw status
show unified-edge ggsn-pgw status gtp-peer
show unified-edge ggsn-pgw status preemption-list
show unified-edge ggsn-pgw status session-state
show unified-edge ggsn-pgw subscribers
show unified-edge ggsn-pgw subscribers charging
show unified-edge ggsn-pgw subscribers traffic-class
show unified-edge ggsn-pgw system
show unified-edge ggsn-pgw system interfaces
show unified-edge ggsn-pgw system interfaces service-mode
show unified-edge sgw
show unified-edge sgw call-rate
show unified-edge sgw call-rate statistics
show unified-edge sgw charging
show unified-edge sgw charging global
show unified-edge sgw charging global statistics
show unified-edge sgw charging local-persistent-storage
show unified-edge sgw charging local-persistent-storage statistics
show unified-edge sgw charging path
show unified-edge sgw charging path statistics
show unified-edge sgw charging path status
show unified-edge sgw charging service-mode
show unified-edge sgw charging transfer
show unified-edge sgw charging transfer statistics
show unified-edge sgw charging transfer status
show unified-edge sgw charging trigger-profile
show unified-edge sgw gtp
show unified-edge sgw gtp peer
show unified-edge sgw gtp peer count
show unified-edge sgw gtp peer history
show unified-edge sgw gtp peer statistics
show unified-edge sgw gtp statistics
show unified-edge sgw idle-mode-buffering
show unified-edge sgw idle-mode-buffering statistics
show unified-edge sgw ip-reassembly
show unified-edge sgw ip-reassembly statistics
show unified-edge sgw resource-manager
show unified-edge sgw resource-manager clients
show unified-edge sgw service-mode
show unified-edge sgw statistics
show unified-edge sgw status
show unified-edge sgw status gtp-peer
show unified-edge sgw status preemption-list
show unified-edge sgw status session-state
show unified-edge sgw subscribers
show unified-edge sgw subscribers charging
show unified-edge sgw system
show unified-edge sgw system interfaces
show unified-edge sgw system interfaces service-mode
<get-mobile-serving-gateway-interface-service-mode>
show unified-edge tdf
show unified-edge tdf aaa
show unified-edge tdf aaa radius
show unified-edge tdf aaa radius client
show unified-edge tdf aaa radius client statistics
<radius-client-statistics>
show unified-edge tdf aaa radius client status
show unified-edge tdf aaa radius network-element
show unified-edge tdf aaa radius network-element statistics
<get-aaa-radius-element-statistics>
show unified-edge tdf aaa radius network-element status
<get-aaa-radius-element-status>
show unified-edge tdf aaa radius server
show unified-edge tdf aaa radius server statistics
radius-server-statistics
show unified-edge tdf aaa radius server status
<get-aaa-radius-server-status>
show unified-edge tdf aaa radius snoop-segment
show unified-edge tdf aaa radius snoop-segment statistics
<radius-snoop-segment-statistics>
show unified-edge tdf aaa statistics
<get-tdf-gateway-aaa-statistics>
show unified-edge tdf address-assignment
show unified-edge tdf address-assignment pool
<get-tdf-gateway-sm-ippool-pool-information>
show unified-edge tdf address-assignment service-mode
<get-tdf-address-assign-service-mode>
show unified-edge tdf address-assignment statistics
<get-tdf-gateway-sm-ippool-statistics>
show unified-edge tdf call-admission-control
show unified-edge tdf call-admission-control statistics
<get-tdf-cac-statistics>
show unified-edge tdf call-rate
show unified-edge tdf call-rate statistics
<get-tdf-call-rate-statistics>
show unified-edge tdf diameter
show unified-edge tdf diameter network-element
show unified-edge tdf diameter network-element statistics
<get-diameter-network-element-statistics>
show unified-edge tdf diameter network-element status
<get-diameter-network-element-status>
show unified-edge tdf diameter pcc-gx
show unified-edge tdf diameter pcc-gx statistics
<get-diameter-statistics-gx>
show unified-edge tdf diameter peer
show unified-edge tdf diameter peer statistics
<get-gateway-diameter-peer-statistics>
show unified-edge tdf diameter peer status
<get-diameter-peer-status>
show unified-edge tdf domain
show unified-edge tdf domain service-mode
<get-mobile-gateways-domain-service-mode>
show unified-edge tdf domain statistics
<get-mobile-gateways-domain-statistics>
show unified-edge tdf resource-manager
show unified-edge tdf resource-manager clients
<get-mobile-gateway-tdf-client-status-information>
show unified-edge tdf service-mode
<get-tdf-gateway-service-mode>
show unified-edge tdf statistics
<get-tdf-statistics>
show unified-edge tdf status
<get-tdf-gateway-status>
show unified-edge tdf status subscriber-state
<get-tdf-gateways-status-state>
show unified-edge tdf subscribers
<get-tdf-gateway-subscribers>
show unified-edge tdf subscribers data-plane
<get-tdf-gateway-subscriber-dataplane-statistics>
show unified-edge tdf subscribers stuck
<get-tdf-gateway-stuck-subscribers>
show unified-edge tdf system
show unified-edge tdf system interfaces
<get-tdf-interfaces-information>
show unified-edge tdf system interfaces service-mode
<get-mobile-tdf-interface-service-mode>
show version
<get-software-information>

show virtual-chassis
show virtual-chassis active-topology
<get-virtual-chassis-active-topology>
show virtual-chassis device-topology
<get-virtual-chassis-device-topology>
show virtual-chassis fast-failover
<get-virtual-chassis-fast-failover>
show virtual-chassis heartbeat
<get-virtual-chassis-heartbeat-information>
show virtual-chassis login
<get-virtual-chassis-login>
show virtual-chassis mode
<get-virtual-chassis-mode-information>
show virtual-chassis protocol
show virtual-chassis protocol adjacency
<get-virtual-chassis-adjacency-information>
show virtual-chassis protocol database
<get-virtual-chassis-database-information>
show virtual-chassis protocol interface
<get-virtual-chassis-interface-information>
show virtual-chassis protocol route
<get-virtual-chassis-route-information>
show virtual-chassis protocol statistics
<get-virtual-chassis-statistics-information>
show virtual-chassis status
<get-virtual-chassis-information>
show virtual-chassis vc-path
<get-virtual-chassis-packet-path>
show virtual-chassis vc-port
<get-virtual-chassis-port-information>
show virtual-chassis vc-port diagnostics
show virtual-chassis vc-port diagnostics optics
<get-virtual-chassis-optics-diagnostics>
show virtual-chassis vc-port lag-hash
<get-virtual-chassis-port-lag-hash-information>
show virtual-chassis vc-port statistics
<get-virtual-chassis-port-statistics>
show vlans
<get-vlan-information>
show vlans operational
<get-operational-vlan-instance-information>
show vlans satellite
<get-satellite-control-bridge-domain>
show vmhost
show vmhost bridge
<get-vmhost-bridge-information>
show vmhost crash
<get-vmhost-crash-information>
show vmhost hardware
<get-vmhost-hardware>
show vmhost information
<get-vmhost-information>
show vmhost logs
<get-vmhost-logs-information>
show vmhost management-if
<get-vmhost-management-if-info>
show vmhost netstat
<get-vmhost-netstat>
show vmhost processes
<get-vmhost-processes-information>
show vmhost resource-usage
<get-vmhost-resource-usage-information>
show vmhost snapshot
<get-vmhost-snapshot-information>
show vmhost status
<get-vmhost-status>
show vmhost uptime
<get-vmhost-uptime>
show vmhost version
<get-vmhost-version-information>

show vpls
show vpls connections
    <get-vpls-connection-information>

show vpls flood
show vpls flood event-queue
    <get-vpls-event-queue-information>

show vpls flood route
show vpls flood route all-ce-flood
    <get-vpls-all-ce-flood-route-information>

show vpls flood route all-flood
    <get-vpls-all-flood-route-information>

show vpls flood route alt-root-flood
    <get-vpls-alt-root-flood-route-information>

show vpls flood route ce-flood
    <get-vpls-ce-flood-route-information>

show vpls flood route mlp-flood
    <get-vpls-mlp-flood-route-information>

show vpls flood route re-flood
    <get-vpls-re-flood-route-information>

show vpls mac-table
    <get-vpls-mac-table>

show vpls mac-table interface
    <get-vpls-interface-mac-table>

show vpls statistics
    <get-vpls-statistics-information>
show vrrp
show vrrp interface
show vrrp track
test interface
test interface fdl-line-loop
test interface fdl-line-loop ansi
test interface fdl-line-loop ansi initiate
test interface fdl-line-loop ansi terminate
test interface fdl-line-loop bellcore
test interface fdl-line-loop bellcore initiate
test interface fdl-line-loop bellcore terminate
test interface fdl-payload-loop
test interface fdl-payload-loop ansi
test interface fdl-payload-loop ansi initiate
test interface fdl-payload-loop ansi terminate
test interface fdl-payload-loop bellcore
test interface fdl-payload-loop bellcore initiate
test interface fdl-payload-loop bellcore terminate
test interface inband-line-loop
test interface inband-line-loop ansi
test interface inband-line-loop ansi initiate
test interface inband-line-loop ansi terminate
test interface inband-line-loop bellcore
test interface inband-line-loop bellcore initiate
test interface inband-line-loop bellcore terminate
test interface inband-line-loop initiate
test interface inband-line-loop terminate
test interface inband-payload-loop
test interface inband-payload-loop ansi
test interface inband-payload-loop ansi initiate
test interface inband-payload-loop ansi terminate
test interface inband-payload-loop bellcore
test interface inband-payload-loop bellcore initiate
test interface inband-payload-loop bellcore terminate
test msdp
test msdp dependent-peers
test msdp rpf-peer
test policy
<
[edit dynamic-profiles routing-instances instance services mobile-ip home-agent enable-service]
[edit logical-systems routing-instances instance services mobile-ip home-agent enable-service]
[edit logical-systems services mobile-ip home-agent enable-service]
[edit routing-instances instance services mobile-ip home-agent enable-service]
[edit services mobile-ip home-agent enable-service]

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160

view-configuration

Can view all of the configuration (not including secrets).

Commands

No associated CLI commands.

Configuration Hierarchy Levels

No associated CLI configuration hierarchy levels and statements.
## RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Understanding Junos OS Access Privilege Levels</th>
<th>118</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Configuring User Permissions with Access Privilege Levels</td>
<td>124</td>
</tr>
<tr>
<td>Example: Configuring User Permissions with Access Privileges for Operational Mode Commands</td>
<td>145</td>
</tr>
<tr>
<td>Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies</td>
<td>160</td>
</tr>
</tbody>
</table>
Configuration Statements

access | 1447
access (Dynamic Access Routes) | 1449
access-internal (Dynamic Access-Internal Routes) | 1451
access-profile | 1453
accounting (System) | 1455
accounting (Access Profile) | 1457
accounting (Access Profile) | 1459
accounting-options | 1461
accounting-order | 1464
accounting-port (RADIUS Server) | 1465
accounting-server | 1466
accounting-stop-on-access-deny | 1468
accounting-stop-on-failure | 1469
active-server-group | 1471
add-interface-text-description | 1473
authentication-profile-name | 1524
authentication-protocol | 1525
authentication-server | 1527
authentication-whitelist | 1528
authorization | 1529
authorization-time-interval | 1530
backoff-factor | 1532
backoff-threshold | 1533
backup-on-failure (Accounting Options) | 1534
bfd | 1535
block-interval | 1537
boot-loader-authentication | 1538
boot-server (NTP) | 1540
boot-server (NTP) | 1541
boot-server (DHCP) | 1542
broadcast | 1543
broadcast | 1545
broadcast-client | 1546
broadcast-client | 1547
ca-name | 1548
certificate-verification | 1553
cache-size | 1552
cache-timeout-negative | 1553
captive-portal | 1554
certificate-verification | 1556
certificates | 1558
certification-authority | 1560
change-type | 1562
civic-based | 1563

ciphers | 1564

circuit-id (DHCP Relay Agent) | 1566

circuit-type | 1569

circuit-type (DHCP Local Server) | 1570

circuit-type (DHCP Relay Agent) | 1572

class (Defining Login Classes) | 1573

class-usage-profile | 1584

classification-key (DHCP Local Server) | 1585

classification-key (DHCP Relay Agent) | 1586

clear-on-abort (DHCP Local Server) | 1588

client-alive-count-max | 1590

client-alive-interval | 1591

client-discover-match (DHCP Local Server) | 1592

client-ia-type | 1594

client-id (DHCP Local Server) | 1595

client-id (DHCP Relay Agent) | 1596

client-identifier (DHCP Client) | 1597

client-identifier (DHCPv6 Client) | 1598

client-list-name | 1599

client-list-name (SNMP) | 1600

client-type | 1601

clients | 1602

coa-immediate-update | 1603

coa-no-override service-class-attribute | 1604

commit-delay | 1605

community (SNMP) | 1606

compress (Accounting Options) | 1607

connection-limit | 1608
dhcpv6-client | 1709

diameter-instance (Diameter Applications) | 1711

disable (802.1X) | 1712

disable (DNSSEC) | 1713

disable (LLDP) | 1714

disable (LLDP-MED) | 1715

disable (LLDP Power Negotiation) | 1716

disable-relay | 1717

dl | 1718

domain (Domain Map) | 1719

domain-name (DHCP) | 1721

domain-name (DHCP Local Server) | 1722

domain-name (DHCP Relay Agent) | 1724

domain-name-server (Routing Instances and Access Profiles) | 1726

domain-name-server-inet (Routing Instances and Access Profiles) | 1727

domain-name-server-inet6 (Routing Instances and Access Profiles) | 1728

domain-search | 1729

dot1x | 1730

drop (DHCP Relay Agent Option) | 1732

dual-stack (DHCP Local Server Overrides) | 1733

dual-stack (DHCP Relay Agent Overrides) | 1734

dual-stack-group (DHCP Local Server) | 1735

dual-stack-group (DHCP Relay Agent) | 1737

dual-stack-interface-client-limit (DHCP Local Server and Relay Agent) | 1740

duplication (Access Profile) | 1741

duplication-filter (Access Profile) | 1742

duplication-vrf (Duplicate Accounting) | 1743

dynamic-pool | 1744

dynamic-profile (DHCP Local Server) | 1746
finger | 1798
fingerprint-hash | 1799
flow-tap-dtcp | 1800
force-discover (DHCP Client) | 1801
format (System Login) | 1802
forward-snoop-clients (DHCP Local Server) | 1803
forward-snoop-clients (DHCP Relay Agent) | 1804
forwarding-class (VoIP) | 1806
forwarding-options (Security) | 1808
ftp | 1810
global (Gx-Plus) | 1811
group (DHCP Local Server) | 1812
group (DHCP Relay Agent) | 1818
group (System Services DHCP) | 1824
guest-vlan | 1828
gx-plus (Gx-Plus) | 1829
health-monitor | 1830
hold-multiplier | 1831
holddown-interval | 1832
host (SSH Known Hosts) | 1833
hostkey-algorithm | 1835
host-name (DHCP Relay Agent) | 1837
http | 1838
https | 1839
ignore-port-bounce | 1840
immediate-update | 1841
include-ipv6 (Gx-Plus) | 1842
include-irb-and-l2 | 1843
infranet-controller | 1846
interface (802.1X) | 1847
interface (Access Control Service) | 1849
interface (Captive Portal) | 1850
interface (DHCP Local Server) | 1851
interface (DHCP Relay Agent) | 1854
interface (LLDP) | 1857
interface (LLDP-MED) | 1859
interface (Static MAC Bypass) | 1861
interface (System Services DHCP) | 1862
interface (VoIP) | 1864
interface-client-limit (DHCP Local Server) | 1866
interface-client-limit (DHCP Relay Agent) | 1868
interface-delete (Subscriber Management or DHCP Client Management) | 1870
interface-description-format | 1871
interface-name (DHCP Local Server) | 1873
interface-profile | 1874
interface-traceoptions (System Services DHCP) | 1875
interfaces (ARP) | 1877
interfaces (Security Zones) | 1878
interval (Accounting Options) | 1879
interval (Access Control Service) | 1880
interval (Health Monitor) | 1881
interval (Health Monitor) | 1882
ip-address-first | 1883
keep-incoming-circuit-id (DHCP Relay Agent) | 1884
keep-incoming-remote-id (DHCP Relay Agent) | 1885
key (Authentication Keychain) | 1886
key-chain (Security) | 1888
key-exchange | 1890
layer2-liveness-detection (Send) | 1892
layer2-unicast-replies | 1894
ldap-url | 1895
lease-time | 1896
lease-time (dhcp-client) | 1897
liveness-detection | 1898
lldp | 1900
lldp | 1902
lldp-configuration-notification-interval | 1905
lldp-med (Ethernet Switching) | 1906
lldp-med-bypass | 1908
lldp-priority | 1909
lldp-tx-fast-init | 1910
local | 1911
local-certificate | 1913
local-server-group (DHCP Relay Agent Option) | 1914
location (DHCP Relay Agent) | 1915
location (LLDP-MED) | 1916
location (SNMP) | 1917
location (System) | 1918
lockout-period | 1920
log | 1921
log-key-changes | 1922
logical-system-name (DHCP Local Server) | 1923
login | 1924
mac-address (DHCP Local Server) | 1927
mac-address (DHCP Relay Agent) | 1929
mac-radius | 1931
macs | 1933
management-address | 1935
master-password | 1936
mau-type | 1938
max-outstanding-requests (Diameter Applications) | 1939
max-pre-authentication-packets | 1940
max-sessions-per-connection | 1941
maximum-certificates | 1942
maximum-hop-count | 1943
maximum-lease-time (DHCP) | 1944
maximum-length | 1945
maximum-lifetime | 1946
maximum-requests | 1947
maximum-time | 1948
message | 1949
method | 1950
mib-profile | 1952
minimum-changes | 1953
minimum-character-changes | 1954
minimum-interval | 1955
minimum-length | 1957
minimum-lifetime | 1958
minimum-lower-cases | 1960
minimum-numerics | 1961
minimum-punctuations | 1962
minimum-receive-interval | 1963
minimum-reuse | 1964
minimum-time | 1965
minimum-upper-cases | 1966
minimum-wait-time | 1967
multi-domain | 1968
multicast-client | 1970
multicast-client | 1971
multiplier | 1972
name-server (Access) | 1973
name-server (System Services) | 1974
nas-ip-address | 1975
nas-port-extended-format | 1976
nas-port-id-format (Subscriber Management) | 1978
nas-port-type (Subscriber Management) | 1980
neighbor-discovery-router-advertisement (Access) | 1982
neighbor-port-info-display | 1983
netbios-snooping | 1985
next-hop (Dynamic Access Routes) | 1986
next-server | 1988
no-adaptation | 1989
no-allow-snooped-clients | 1990
no-bind-on-request (DHCP Relay Agent) | 1992
no-listen | 1994
no-mac-table-binding (802.1X) | 1995
no-passwords | 1996
no-public-keys | 1997
no-reauthentication | 1998
no-tagging | 1999
no-tcp-forwarding | 2000
no-vlan-interface-name | 2001
nonpersistent | 2003
nonvolatile | 2004
ntp | 2005
quiet-period  |  2131
quiet-period (Captive Portal)  |  2132
radius  |  2133
radius (Access Profile)  |  2134
radius (System)  |  2138
radius-disconnect (DHCP Local Server)  |  2139
radius-options  |  2141
radius-options (802.1X)  |  2142
radius-options (Access)  |  2143
radius-options (System)  |  2144
radius-server  |  2146
radius-server  |  2148
radius-server  |  2154
radius-server (System)  |  2156
radsec  |  2157
radsec-destination  |  2159
rapid-commit (DHCPv6 Client)  |  2160
rapid-commit (DHCPv6 Local Server)  |  2161
rate-limit  |  2162
reauthenticate (DHCP Local Server)  |  2164
reauthentication  |  2167
reconfigure (DHCP Local Server)  |  2168
reconfigure (DHCP Local Server)  |  2170
redirect-url  |  2172
regex-additive-logic  |  2174
relay-agent-interface-id (DHCP Local Server)  |  2176
relay-agent-interface-id (DHCPv6 Relay Agent)  |  2177
relay-agent-remote-id (DHCP Local Server)  |  2179
relay-agent-remote-id (DHCPv6 Relay Agent Username)  |  2181
session-mode | 2265
sftp-server | 2266
short-cycle-protection (DHCP Local Server and Relay Agent) | 2267
single-connection | 2269
sip-server | 2270
size | 2271
snmp | 2272
source-address (NTP, RADIUS, System Logging, or TACACS+) | 2279
source-address (SRC Software) | 2280
source-address-giaddr | 2281
source-classes | 2282
source-ip-change (Forwarding Options) | 2283
ssh (System Services) | 2284
ssh-known-hosts | 2286
ssh-known-hosts | 2287
ssl-renegotiation | 2288
start-time (Accounting) | 2289
start-time (Authentication Key Transmission) | 2290
static (Protocols 802.1X) | 2292
static-binding | 2294
static-subscribers | 2295
statistics (Access Profile) | 2296
statistics-service | 2297
strict (DHCP Local Server) | 2298
sub-prefix-length | 2299
subscriber-management-helper | 2300
supplicant | 2301
supplicant-timeout | 2303
system-generated-certificate | 2304
transfer-interval | 2363
transmit-delay (LLDP) | 2364
transmit-delay | 2365
transmit-interval | 2367
transmit-period | 2368
trap-group | 2369
trap-options | 2371
trigger (DHCP Local Server) | 2373
tries-before-disconnect | 2375
trust-option-82 | 2376
trusted-key | 2377
uac-policy | 2378
uac-service | 2379
uac-service | 2380
unattended-boot | 2381
unified-access-control | 2382
update-interval | 2383
update-router-advertisement | 2385
update-server | 2386
update-server (dhcp-client) | 2387
update-server (dhcpv6-client) | 2388
usb-control | 2389
use-interface | 2390
use-interface-description | 2391
use-primary (DHCP Local Server) | 2394
use-primary (DHCP Relay Agent) | 2396
use-vlan-id | 2398
use-vlan-id (DHCP Relay Agent) | 2400
user (Access) | 2402
user-defined-option-82 | 2404
user-id | 2406
user-keepalive | 2407
user-prefix (DHCP Local Server) | 2408
username-include (DHCP Local Server) | 2410
username-include (DHCP Relay Agent) | 2412
vendor-id | 2414
vendor-option | 2415
vendor-option | 2416
version (BFD) | 2418
version (SNMP) | 2420
versioning | 2421
view-configuration | 2421
vlan (VoIP) | 2423
vlan-assignment | 2424
vlan-name-tlv-option | 2426
voip | 2427
vpn (Forwarding Options) | 2428
wait-for-acct-on-ack (Access Profile) | 2429
watchdog | 2430
web-management | 2431
web-management (System Processes) | 2432
web-management (System Services) | 2433
what | 2438
wins-server (System) | 2440
xnm-clear-text | 2441
xnm-ssl | 2442
access

Syntax

access {
    address-assignment
    pool pool-name
    address-pool pool-name
    profile profile-name {
        accounting (Access Profile) {
            accounting-stop-on-access-deny;
            accounting-stop-on-failure;
            (authentication-order (Access Profile) (ldap radius | none);
            order (radius | none);
        }
        radius {
            accounting-server [server-addresses];
            authentication-server [server-addresses];
        }
    }
}

Hierarchy Level

[edit]

Release Information

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

Description

Configure authentication, authorization, and accounting (AAA) services.

The remaining statements are explained separately. See CLi Explorer.

NOTE: The [edit access] hierarchy is not available on QFabric systems.

Default

Not enabled
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

| Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438 |
access (Dynamic Access Routes)

Syntax

```
access {
    route prefix {
        next-hop next-hop;
        metric route-cost;
        preference route-distance;
        tag route-tag;
        tag2 route-tag2;
    }
}
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name],
[edit dynamic-profiles profile-name routing-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.

Description

Dynamically configure access routes in a dynamic client profile.

NOTE: Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support. We recommend that you do not use access-internal routes. If you configure the access-internal statement in the dynamic profile, it is ignored. The subscriber’s address is stored in the session database entry before the dynamic profile installs the framed route, enabling the next-hop address to be resolved when it is not explicitly specified in the Framed-Route RADIUS attribute [22] or Framed-IPv6-Route attribute [99].

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.
routeing-control—To add this statement to the configuration.
### Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support.</td>
</tr>
</tbody>
</table>

### RELATED DOCUMENTATION

- *Configuring Dynamic Access Routes for Subscriber Management*
access-internal (Dynamic Access-Internal Routes)

Syntax

```
access-internal {
  route subscriber-ip-address {
    qualified-next-hop underlying-interface {
      mac-address address;
    }
  }
}
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name],
[edit dynamic-profiles routing-options]
```

Release Information

Statement introduced in Junos OS Release 9.5.

Description

(Releases earlier than Junos OS Release 15.1) Dynamically configure access-internal routes in a dynamic client profile. Access-internal routes are optional, but are used instead of access routes if the next-hop address is not specified in the Framed-Route Attribute [22] for IPv4 or the Framed-IPv6-Route attribute [99] for IPv6.

NOTE: Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support. We recommend that you do not use access-internal routes. If you configure the `access-internal` statement in the dynamic profile, it is ignored. The subscriber’s address is stored in the session database entry before the dynamic profile installs the framed route, enabling the next-hop address to be resolved when it is not explicitly specified in the Framed-Route RADIUS attribute (22) or Framed-IPv6-Route attribute [99].

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Release History Table

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Starting in Junos OS Release 15.1, we recommend that you use only access routes for framed route support.</td>
</tr>
</tbody>
</table>

RELATED DOCUMENTATION

Configuring Dynamic Access-Internal Routes for DHCP and PPP Subscribers
access-profile

Syntax

access-profile profile-name;

Hierarchy Level

[edit],
[edit forwarding-options dhcp-relay]
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name]
[edit forwarding-options dhcp-relay dhcpv6]
[edit forwarding-options dhcp-relay dhcpv6 group group-name]
[edit logical-systems logical-system-name routing-instances routing-instance-name]
[edit interfaces interface-name auto-configure vlan-ranges],
[edit interfaces interface-name auto-configure stacked-vlan-ranges],
[edit routing-instances routing-instances-name]
[edit system services dhcp-local-server]
[edit system services dhcp-local-server group group-name]
[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server dhcpv6 group group-name]
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
After you have created the access profile that specifies authentication and accounting parameters, you must specify where the profile is used. Authentication and accounting will not run unless you specify the profile. You can attach access profiles globally at the [edit] hierarchy level, or you can apply them to DHCP clients or subscribers, VLANs, or to a routing instance.

Options
profile-name—Name of the access profile that you configured at the [edit access profile name] hierarchy level.

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

RADIUS Servers and Parameters for Subscriber Access

Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution

Configuring Access Components for the PPPoE Wholesale Network Solution
accounting (System)

Syntax

```
accounting {
    events [login change-log interactive-commands];
    destination {
        radius {
            server {
                server-address {
                    accounting-port port-number;
                    retry number;
                    routing-instance routing-instance;
                    secret password;
                    source-address address;
                    timeout seconds;
                }
            }
        }
        tacplus {
            server {
                server-address {
                    port port-number;
                    routing-instance routing-instance;
                    secret password;
                    single-connection;
                    timeout seconds;
                }
            }
        }
    }
    enhanced-avs-max <number>;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `source-address-inet6` statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

**Description**
Configure audit of TACACS+ or RADIUS authentication events, configuration changes, and interactive commands. Auditing these factors helps you track network usage for auditing and billing purposes.

The remaining statements are explained separately.

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

**RELATED DOCUMENTATION**
- Configuring RADIUS System Accounting | 255
- Configuring TACACS+ System Accounting | 278
- enhanced-avs-max | 1757
- System Management Configuration Statements
accounting (Access Profile)

Syntax

```
accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order (radius | none);
}
```

Hierarchy Level

```
[edit access profile profile-name]
```

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

Description
Configure the authentication order for authentication, authorization, and accounting (AAA) services.

Default
Not enabled

Options
- none—Use no authentication for specified subscribers.
- radius—Use RADIUS authentication for specified subscribers.

The remaining statements are explained separately. See CLI Explorer.

**NOTE:** The [edit access] hierarchy is not available on QFabric systems.

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

RELATED DOCUMENTATION
accounting (Access Profile)

Syntax

```
accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    address-change-immediate-update;
    ancp-speed-change-immediate-update;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    duplication-filter;
    duplication-vrf {
        access-profile-name profile-name;
        vrf-name vrf-name;
    }
    immediate-update;
    order [accounting-method];
    send-acct-status-on-config-change
    statistics (time | volume-time);
    update-interval minutes;
    wait-for-acct-on-ack;
}
```

Hierarchy Level

```
[edit access profile profile-name]
```

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

Description
Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting
- Understanding RADIUS Accounting Duplicate Reporting
accounting-options

Syntax

accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name;
    }
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      input-bytes;
      input-errors;
      input-multicast;
      input-packets;
      input-unicast;
      output-bytes;
      output-errors;
      output-multicast;
      output-packets;
      output-unicast;
    }
  }
}
rpf-check-bytes;
rpf-check-packets;
rpf-check6-bytes;
rpf-check6-packets;
unsupported-protocol;
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
}
Hierarchy Level

[edit]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure options for accounting statistics collection.

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

RELATED DOCUMENTATION

- Understanding RADIUS Accounting | 254
- Juniper-Switching-Filter VSA Match Conditions and Actions | 251
- Configuring RADIUS System Accounting | 255
- Configuring Remote Template Accounts for User Authentication | 212
- Configuring Local User Template Accounts for User Authentication | 210
accounting-order

Syntax

accounting-order (radius | [accounting-order-data-list]);

Hierarchy Level

[edit access profile profile-name]

Release Information
Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Specify the order in which accounting methods are used.

Options
radius—Use the RADIUS accounting method.

[accounting-order-data-list]—Set of data listing the accounting order to be used, enclosed in brackets. This can be any combination of accounting methods, up to and including a list of the entire accounting order.

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

RELATED DOCUMENTATION

Configuring the Accounting Order
accounting-port (RADIUS Server)

Syntax

```
accounting-port port-number;
```

Hierarchy Level

```
[edit system accounting destination radius server server-address],
[edit system radius-server server-address]
```

Release Information
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure the accounting port number on which to contact the RADIUS server.

Options

- `number`—Port number on which to contact the RADIUS server.

Default: 1813

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
- Configuring RADIUS System Accounting | 255
accounting-server

Syntax

```
accounting-server[server-addresses];
```

Hierarchy Level

```
[edit access profile profile-name radius]
```

Release Information

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

Description

Configure the Remote Authentication Dial-In User Service (RADIUS) server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Default

Not enabled

Options

`server-addresses`—One or more addresses of RADIUS authentication servers.

NOTE: The `[edit access]` hierarchy is not available on QFabric systems.

Required Privilege Level

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

RELATED DOCUMENTATION

- `show network-access aaa statistics authentication` | 2714
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
accounting-stop-on-access-deny

Syntax

accounting-stop-on-access-deny;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

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

Description

Configure the authentication order for authentication, authorization, and accounting (AAA) services to send an Acct-Stop message if the AAA server denies access to a supplicant.

NOTE: The [edit access] hierarchy is not available on QFabric systems.

Default

Not enabled

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
show network-access aaa statistics authentication | 2714
accounting-stop-on-failure

Syntax

accounting-stop-on-failure;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

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

Description

Configure RADIUS accounting to send an Acct-Stop message when a subscriber session has been successfully authenticated and authorized, but then fails before an Acct-Start message is sent. By default, an Acct-Stop message is sent only if an Acct-Start message has been exchanged with the accounting server.

Consider a situation where RADIUS address pools are used to assign IP/IPv6 addresses. After a subscriber session is successfully authenticated, the RADIUS server authorizes the session by assigning an IP address from the RADIUS address pool and conveying that address in the Framed-IP-Address attribute. If a negotiation failure occurs at this point, the session is terminated before activating. The Acct-Start message is never sent because it is initiated by session activation. By default, an Acct-Stop message cannot be sent because the Acct-Start is never sent. However, if the acct-stop-on-failure statement is configured, the negotiation failure causes the Acct-Stop message to be sent, which explicitly notifies the RADIUS server that the session is disconnected and that it can free the allocated IP address back to the pool.

NOTE: The [edit access] hierarchy is not available on QFabric systems.

Default

Disabled

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.
## RELATED DOCUMENTATION

| Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400 |
| Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438 |
| Understanding 802.1X and RADIUS Accounting on Switches | 435 |
| Understanding RADIUS Accounting | 254 |
active-server-group

Syntax

active-server-group server-group-name <allow-server-change>;

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name],

Release Information
Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
allow-server-change option added in Junos OS Release 16.2R1.

Description
Apply a DHCP relay agent configuration to the named group of DHCP server addresses. The server group itself is configured with the server-group statement. You can apply an active server group globally or for specific groups of interfaces, configured with the group statement. An active server group applied to an interface group overrides a global configuration.

Options
allow-server-change—(Optional) (DHCPv4 only) Enable the relay agent to accept and forward a DHCP request (renew or rebind) ACK message to the client from any DHCP local server in the active server
group. Starting in Junos OS Release 18.4R1, this option also applies to DHCP information request (DHCPINFORM) ACK messages.

**Default:** Forward ACK messages from only the original binding server.

*server-group-name*—Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- [Extended DHCP Relay Agent Overview](#) | 792
- [Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups](#) | 850
- [Configuring Group-Specific DHCP Relay Options](#) | 856
add-interface-text-description

Syntax

```
add-interface-text-description;
```

Hierarchy Level

```
[edit protocols dot1x authenticator radius-options]
```

Release Information

Statement introduced in Junos OS Release 18.4R1 for EX Series switches.

Description

Configure the NAS-Port-ID attribute to include the text description of the interface to which a RADIUS client is connected. The NAS-Port-ID is a RADIUS attribute that is included in the Access-Request message sent from a client to the RADIUS server. By default, the attribute is populated with the name of the logical interface. Including the text description provides more information to the RADIUS server, which can use the information to assign the client to a different VLAN or apply a firewall filter for authentication.

The text description of the interface is configured under the `[edit interfaces interface-name]` hierarchy level. When you configure the `add-interface-text-description` option under the `[edit protocols dot1x authenticator radius-options]` hierarchy level, the text description is appended to the interface name in the Access-Request message in the format `interface-name#interface-text-description`.

If there is a text description configured for the logical interface, it is used in the NAS-Port-ID; otherwise, the text description for the physical interface is used. If neither is configured then the NAS-Port-ID will only contain the interface name.

There is no character limit for the interface text description; however, the total length of the NAS-Port-ID with the interface name and description combined is restricted to 253 characters. If the total length exceeds 253 characters, the description is truncated.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding 802.1X and RADIUS Accounting on Switches | 435
- Understanding Dynamic Filters Based on RADIUS Attributes | 405
address (Access Control Service)

Syntax

```
address ip-address;
```

Hierarchy Level

```
[edit services unified-access-control infranet-controller]
```

Release Information
Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description
Specify the address through which the switch will connect to the Junos Pulse Access Control Service.

Options

- `ip-address`—Specify the IP address of the NAC device.

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
address-assignment (Access)

Syntax

```plaintext
address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-name;
    pool pool-name {
        family {
            inet {
                dhcp-attributes {
                    boot-file boot-file-name;
                    boot-server boot-server-name;
                    domain-name domain-name;
                    grace-period seconds;
                    maximum-lease-time (seconds | infinite);
                    name-server ipv4-address;
                    netbios-node-type (b-node | h-node | m-node | p-node);
                    next-server next-server-name;
                    option dhcp-option-identifier-code {
                        array {
                            byte [8-bit-value];
                            flag [false | off | on | true];
                            integer [32-bit-numeric-values];
                            ip-address [ip-address];
                            short [signed-16-bit-numeric-value];
                            string [character string value];
                            unsigned-integer [unsigned-32-bit-numeric-value];
                            unsigned-short [16-bit-numeric-value];
                        }
                        byte 8-bit-value;
                        flag (false | off | on | true);
                        integer 32-bit-numeric-values;
                        ip-address ip-address;
                        short signed-16-bit-numeric-value;
                        string character string value;
                        unsigned-integer unsigned-32-bit-numeric-value;
                        unsigned-short 16-bit-numeric-value;
                    }
                }
            }
        }
    }
}
```

circuit-id match-value {
    range range-name;
}
remote-id match-value {
    range range-name;
}
propagate-ppp-settings [interface-name];
propagate-settings interface-name;
arouter ipv4-address;
server-identifier ip-address;
sip-server {
    ip-address ipv4-address;
    name sip-server-name;
}
tftp-server server-name;
wins-server ipv4-address;
} host hostname {
    hardware-address mac-address;
    ip-address reserved-address;
}
network network address;
range range-name {
    high upper-limit;
    low lower-limit;
}
excluded-range range-name {
    high upper-limit;
    low lower-limit;
}
xauth-attributes {
    primary-dns ip-address;
    primary-wins ip-address;
    secondary-dns ip-address;
    secondary-wins ip-address;
}
inet6 {
  dhcp-attributes {
    dns-server ipv6-address;
    grace-period seconds;
    maximum-lease-time (seconds | infinite);
    option dhcp-option-identifier-code {
      array {
        byte [8-bit-value];
        flag [false] off [on] [true];
        integer [32-bit-numeric-values];
        ip-address [ip-address];
        short [signed-16-bit-numeric-value];
        string [character string value];
        unsigned-integer [unsigned-32-bit-numeric-value];
        unsigned-short [16-bit-numeric-value];
      }
      byte 8-bit-value;
      flag (false | off | on | true);
      integer 32-bit-numeric-values;
      ip-address ip-address;
      short signed-16-bit-numeric-value;
      string character string value;
      unsigned-integer unsigned-32-bit-numeric-value;
      unsigned-short 16-bit-numeric-value;
    }
    propagate-ppp-settings [interface-name];
    sip-server-address ipv6-address;
    sip-server-domain-name domain-name;
  }
  prefix ipv6-network-prefix;
  range range-name {
    high upper-limit;
    low lower-limit;
    prefix-length delegated-prefix-length;
  }
  excluded-range range-name
    high upper-limit;
    low lower-limit;
  }
}
link pool-name;
}
Hierarchy Level

[edit access]

Release Information
Statement introduced in Junos OS Release 10.4 for SRX300, SRX320, SRX340, SRX345, SRX550HM devices.

Description
The address-assignment pool feature enables you to create IPv4 and IPv6 address pools that different client applications can share. For example, multiple client applications, such as DHCPv4 or DHCPv6, can use an address-assignment pool to provide addresses for their particular clients.

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

RELATED DOCUMENTATION

Dynamic VPN Overview
address-assignment (Address-Assignment Pools)

Syntax

```
address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
        active-drain;
        family family {
            dhcp-attributes {
                protocol-specific attributes;
            }
            excluded-address ip-address;
            excluded-range name low minimum-value high maximum-value;
            host hostname {
                hardware-address mac-address;
                ip-address ip-address;
            }
            network ip-prefix/<prefix-length>;
            prefix ipv6-prefix;
            range range-name {
                high upper-limit;
                low lower-limit;
                prefix-length prefix-length;
            }
        }
        hold-down;
        link pool-name;
    }
}
```

Hierarchy Level

[edit access]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure address-assignment pools that can be used by different client applications.

**NOTE:** Support for subordinate statements is platform-specific. See individual statement topics for support information.

**Options**

**abated-utilization**—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCP address pools or linked set of address pools. No SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

**Values:** *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

**abated-utilization-v6**—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCPv6 address pools or linked set of address pools. No SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

**Values:** *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

**high-utilization**—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCP address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

**Values:** *percentage*—Percentage used to generate a trap. Range: 2 through 99.

**high-utilization-v6**—(ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCPv6 address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

**Values:** *percentage*—Percentage used to generate a trap. Range: 2 through 99.

**neighbor-discovery-router-advertisement**—(M Series, MX Series, SRX Series, T Series only) Configure the name of the address-assignment pool used to assign the router advertisement prefix.

**Values:** *ndra-pool-name*—Name of the address-assignment pool.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.
RELATED DOCUMENTATION

Address-Assignment Pools Overview

Address-Assignment Pool Configuration Overview

Configuring an Address-Assignment Pool for L2TP LNS with Inline Services

Configuring Address-Assignment Pool Usage Threshold Traps

Configuring an Address-Assignment Pool Used for Router Advertisements
address-change-immediate-update

Syntax

```
address-change-immediate-update;
```

Hierarchy Level

```
[edit access profile profile-name accounting]
```

Release Information


Description

Configure the router to send an Interim-Accounting message to the RADIUS server immediately after on-demand IPv4 allocation and de-allocation.

Changes to this setting take effect for new subscriber logins. Existing subscribers are not impacted by this change except when the AAA daemon restarts.

Default

This functionality is disabled by default.

Required Privilege Level

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

RELATED DOCUMENTATION

- Enabling Immediate Interim Accounting Messages for On-Demand IPv4 Address Changes
- Conserving IPv4 Addresses for Dual-Stack PPP Subscribers Using On-Demand IPv4 Address Allocation
address-pool

Syntax

```
address-pool pool-name {
    address address-or-prefix;
    address-range <low lower-limit> <high upper-limit>;
}
```

Hierarchy Level

```
[edit access]
```

Release Information

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

Description

Allocate IP addresses for clients.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options

pool-name—Name assigned to an address pool.

address—(EX Series, M Series, PTX Series, T Series only) Configure the IP address or prefix value for clients.

Values: address-or-prefix—An address or prefix value.

address-range—Configure the address range.

Values:

- high upper-limit—Upper limit of an address range.
- low lower-limit—Lower limit of an address range.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.
RELATED DOCUMENTATION

Configuring the Address Pool for L2TP Network Server IP Address Allocation
address-pool (Access)

Syntax

```
address-pool pool-name {
    address address or address prefix;
    address-range {
        high upper-limit;
        low lower-limit;
        mask network-mask;
    }
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-wins IP address;
}
```

Hierarchy Level

[edit access]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Create an address-pool for L2TP clients.

Options
- **pool-name**—Name assigned to the address-pool.
- **address**—Configure subnet information for the address-pool.
- **address-range**—Defines the address range available for clients.
- **primary-dns**—Specify the primary-dns IP address.
- **secondary-dns**—Specify the secondary-dns IP address.
- **primary-wins**—Specify the primary-wins IP address.
- **secondary-wins**—Specify the secondary-wins IP address.

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

access-control | 1040
**address-protection**

**Syntax**

```plaintext
address-protection {
  reassign-on-match;
}
```

**Hierarchy Level**

```plaintext
[edit access],
[edit logical-systems logical-system-name routing-instances routing-instance-name access]
```

**Release Information**

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 on EX Series switches.
`reassign-on-match` option added in Junos OS Release 18.4R1.

**Description**

Prevent IPv4 addresses and IPv6 prefixes from being assigned to more than one subscriber session when you use AAA to supply IPv4 addresses.

For IPv4:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IP-Address*
- *Framed-Pool*

The router then takes one of the following actions:

- If an address matches an address in an address pool, the address is taken from the pool, provided it is available.
- If the address is already in use, it is rejected as unavailable.

For IPv6:

If enabled, the router checks the following attributes received from external servers:

- *Framed-IPv6-Prefix*
- *Framed-IPv6-Pool*

The router then takes one of the following actions:
• If a prefix matches a prefix in an address pool, the prefix is taken from the pool, provided it is available.

• If the prefix is already in use, it is rejected as unavailable.

• If the prefix length requested from the external server does not exactly match the pool's prefix length, the authentication request is denied. If configured, the Acct-Stop message includes the cause for termination.

Options
reassign-on-match—Enable reassignment of an address from an existing subscriber to a new subscriber requesting that address. The address in use must not be part of a locally configured pool and address protection must be enabled. The request from the new subscriber is still rejected, but the existing subscriber is sent a disconnect request to begin the logout process. This enables the new subscriber to renegotiate and be assigned that IP address.

If the requested address is in a locally configured pool, the existing subscriber is not disconnected.

NOTE: This option is not supported for IPv6.

Default: Rejects the address request from the new subscriber; the existing subscriber remains intact with the IP address.

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

RELATED DOCUMENTATION

Configuring Duplicate IPv4 Address Protection for AAA
Configuring Duplicate IPv6 Prefix Protection for Router Advertisement
advertisement-interval

Syntax

advertisement-interval seconds;

Hierarchy Level

[edit protocols lldp],
[edit routing-instances routing-instance-name protocols lldp]

Release Information

Statement introduced in Junos OS Release 9.6 for MX Series and T Series routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure an interval for LLDP advertisement.

For switches configured for Link Layer Discovery Protocol, configure the frequency at which LLDP advertisements are sent.

The advertisement-interval value must be greater than or equal to four times the transmit-delay value, or an error will be returned when you attempt to commit the configuration.

NOTE: The default value of transmit-delay is 2 seconds. If you configure the advertisement-interval as less than 8 seconds and you do not configure a value for transmit-delay, the default value of transmit-delay is automatically changed to 1 second in order to satisfy the requirement that the advertisement-interval value must be greater than or equal to four times the transmit-delay value.

Default

Disabled.

Options

seconds—Interval between LLDP advertisement.

Default: 30
Range: 5 through 32768
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

*Configuring LLDP*

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp</td>
<td>2680</td>
</tr>
</tbody>
</table>

*Configuring LLDP (CLI Procedure) | 654

*Understanding LLDP and LLDP-MED on EX Series Switches | 661

*transmit-delay | 2365

*Understanding LLDP | 653*
agent-address

Syntax

agent-address outgoing-interface;

Hierarchy Level

[edit snmp trap-options]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series and EX4600.

Description
Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is `outgoing-interface`, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Options

`outgoing-interface`—Value of the agent address of all SNMPv1 traps generated by this router or switch. The `outgoing-interface` option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

Default: disabled (the agent address is not specified in SNMPv1 traps).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Agent Address for SNMP Traps
algorithm (Authentication Keychain)

Syntax

```
algorithm (hmac-sha-1 | md5);
```

Hierarchy Level

```
[edit security authentication-key-chains key-chain key-chain-name key key]
```

Release Information
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the authentication algorithm for IS-IS.

Options
- **hmac-sha-1**—96-bit hash-based message authentication code (SHA-1).
- **md5**—Message digest 5.

Default: md5

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

RELATED DOCUMENTATION

Example: Configuring Hitless Authentication Key Rollover for IS-IS
Understanding Hitless Authentication Key Rollover for IS-IS
allow-no-end-option (DHCP Relay Agent)

Syntax
allow-no-end-option;

Hierarchy Level
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 14.1X53.

Description
Enable a DHCP relay agent to process packets sent from clients without DHCP Option-255 (end-of-options).

The default behavior in Junos OS is to drop packets that do not include Option 255. To override this default behavior, configure the allow-no-end-option CLI statement at the [edit forwarding-options dhcp-relay overrides] hierarchy level.

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

RELATED DOCUMENTATION
Extended DHCP Relay Agent Overview | 792
Overriding the Default DHCP Relay Configuration Settings | 803
DHCP Snooping Support | 898
allow-snooped-clients

Syntax

allow-snooped-clients;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 10.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.

Description
Explicitly enable DHCP snooping support on the DHCP relay agent.

Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly enable snooping support on the router for DHCPv6 relay agent.

Default
DHCP snooping is disabled by default.

NOTE: On EX4300 and EX9200 switches, the allow-snooped-clients statement is enabled by default at the [edit forwarding-options dhcp-relay overrides] hierarchy level.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
## RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>Overriding the Default DHCP Relay Configuration Settings</td>
<td>803</td>
</tr>
<tr>
<td>DHCP Snooping Support</td>
<td>898</td>
</tr>
<tr>
<td>Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent</td>
<td>902</td>
</tr>
</tbody>
</table>
always-write-giaddr

Syntax

always-write-giaddr;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.

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

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview | 792
dhcp-relay | 1665
always-write-option-82

Syntax

always-write-option-82;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.

- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

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

Using DHCP Relay Agent Option 82 Information | 739
Extended DHCP Relay Agent Overview | 792
always-write-option-82

Syntax

```
always-write-option-82 {
  apply-groups;
  apply-groups-except;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides]
```

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

Description

Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. Using this option allows the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to the DHCP packets, the DHCP relay agent clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.

- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, the DHCP relay agent clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

Required Privilege Level

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

RELATED DOCUMENTATION

- replace-ip-source-with (DHCP Relay Agent) | 2192
- overrides (DHCP Relay Agent) | 2050
ancp-speed-change-immediate-update (ANCP)

Syntax

```plaintext
ancp-speed-change-immediate-update;
```

Hierarchy Level

```
[edit access profile profile-name accounting]
```

Release Information
Statement introduced in Junos OS Release 13.3.

Description
Configure AAA to generate immediate interim accounting updates to the RADIUS server in response to ANCP agent notifications of rate changes on subscriber access lines.

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

RELATED DOCUMENTATION

- Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications
- Configuring Per-Subscriber Session Accounting
- Configuring the ANCP Agent
announcement

Syntax

```
announcement text;
```

Hierarchy Level

```
[edit system login]
```

Release Information

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

Description

Configure a system login announcement. This announcement appears after a user logs in.

Options

text—Text of the announcement. If the text contains any spaces, enclose it in quotation marks.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration

RELATED DOCUMENTATION

Configuring Junos OS to Display a System Login Announcement | 76

message | 1949
archival

Syntax

```
archival {
    configuration {
        archive-sites {
            file://<path>/<filename>;
            ftp://username@host:<port>url-path password password;
            http://username@host:<port>url-path password password;
            pasvftp://username@host:<port>url-path password password;
            scp://username@host:<port>url-path password password;
        }
        transfer-interval interval;
        transfer-on-commit;
        routing-instance routing-instance;
    }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

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

Description

Configure copying of the currently active configuration to an archive site. An archive site can be a file, or an FTP, HTTP, passive FTP, or SCP location.

Options

configuration—Configure the router or switch to periodically transfer its currently active configuration (or after each commit). Parameters include archive-sites, transfer-interval, and transfer-on-commit.

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.
archive-sites—Specify where to transfer the current configuration files. When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example:
"scp://username:<password>@[ipv6-host-address]<:port>/url-path".

If you specify more than one archive site, the router or switch attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails. The destination filename is saved in the following format, where n corresponds to the number of the compressed configuration rollback file that has been archived:

```
router-name_YYYYMMDD_HHMMSS_juniper.conf.n.gz
```

NOTE: The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.

**transfer-interval**—The frequency, in minutes, for transferring the current configuration to an archive site. Valid intervals are 15 to 2880 minutes.

**transfer-on-commit**—Configure the router or switch to transfer its currently active configuration to an archive site each time you commit a candidate configuration.

**routing-instance**—Defines the routing instance through which a server is reachable.

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

**RELATED DOCUMENTATION**

Back up Configurations to an Archive Site
archive-sites

Syntax

```
archive-sites {
    site-name;
}
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format `router-name_log-filename_timestamp`.

To delete an archive site, use the `delete` command instead of `set`.

Options

- **site-name**: Any valid FTP/SCP URL to a destination.

Required Privilege Level

- **snmp**: To view this statement in the configuration.
- **snmp-control**: To add this statement to the configuration.

RELATED DOCUMENTATION

- **Configuring Archive Sites**
attempts (DHCP Local Server)

Syntax

```
attempts attempt-count;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Options

- **attempt-count**—Maximum number of attempts.

Range: 1 through 10
Default: 8

**Required Privilege Level**

system—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

| Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844 |
| Configuring Dynamic Reconfiguration Attempts for DHCP Clients | 847 |
attributes (RADIUS Attributes)

Syntax

attributes {
  exclude {
    attribute-name packet-type;
    standard-attribute number {
      packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
    }
    vendor-id id-number {
      vendor-attribute vsa-number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
      }
    }
  }
  ignore {
    dynamic-iflset-name;
    framed-ip-netmask;
    idle-timeout;
    input-filter;
    logical-system-routing-instance;
    output-filter;
    session-timeout;
    standard-attribute number;
    vendor-id id-number {
      vendor-attribute vsa-number;
    }
  }
}

Hierarchy Level

[edit access profile profile-name radius]

Release Information

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

Description

Specify how the router or switch processes RADIUS attributes.

Options
**exclude**—Configure the router or switch to exclude the specified attributes from being sent in the specified type of RADIUS message. Exclusion can be useful, for example, for attributes that do not change values over the lifetime of a subscriber. By not sending these attributes, you reduce the packet size without losing information. Contrast this behavior with that provided by the **ignore** statement.

The options for this statement are explained separately. Click the linked statement for details.

**ignore**—Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. Standard attributes and VSAs received in RADIUS messages take precedence over internally provisioned attribute values. Ignoring the attributes enables your internally provisioned values to be used instead. Contrast this behavior with that provided by the **exclude** statement.

Starting in Junos OS Release 18.1R1, you can specify RADIUS standard attributes with the attribute number. You can specify vendor-specific attributes (VSAs) with the IANA-assigned vendor ID and the VSA number. With this flexible configuration method, you can configure any standard attribute and VSA supported by your platform to be ignored. The configuration has no effect if you can configure unsupported attributes, vendors, and VSAs.

The legacy method allows you to configure only those attributes and VSAs for which the statement syntax includes a specific option. Consequently, you can use the legacy method to ignore only a subset of all attributes that can be received in Access-Accept messages.

**Values:**

- **dynamic-ifset-name**—Ignore Juniper Networks VSA 26-130, Qos-Set-Name.
- **framed-ip-netmask**—Ignore RADIUS attribute 9, Framed-IP-Netmask.
- **idle-timeout**—Ignore RADIUS attribute 28, Idle-Timeout.
- **input-filter**—Ignore Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **logical-system-routing-instance**—Ignore Juniper Networks VSA 26-1.
- **output-filter**—Ignore Juniper Networks VSA 26-11, Egress-Policy-Name.
- **session-timeout**—Ignore RADIUS attribute 27, Session-Timeout.
- **standard-attribute number**—RADIUS standard attribute number supported by your platform. You can enclose multiple values in square brackets to specify a list of attributes. If you configure an unsupported attribute, that configuration has no effect. Range: 1 through 255.
- **vendor-attribute vsa-number**—Number identifying a VSA belonging to the specified vendor; both must be supported by your platform. You can enclose multiple values in square brackets to specify a list of VSAs. If you configure an unsupported VSA, that configuration has no effect. Range: 1 through 255.
- **vendor-id id-number**—IANA vendor ID supported by your platform. If you configure an unsupported vendor ID, that configuration has no effect. Range: 1 through 16777215.
The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

- RADIUS Servers and Parameters for Subscriber Access
- Standard and Vendor-Specific RADIUS Attributes
- AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS
- AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS
authenticator

Syntax

authenticator {
    authentication-profile-name access-profile-name;
    interface (all | [ interface-names ]) { 
        disable;
        guest-vlan ( vlan-id | vlan-name);
        lldp-med-bypass;
        mac-radius <restrict>;
        maximum-requests number;
        no-reauthentication;
        quiet-period seconds;
        reauthentication interval;
        retries (802.1X) number;
        server-fail (deny | permit | use-cache | vlan-id | vlan-name);
        server-reject-vlan (vlan-id | vlan-name) {
            eapol-block;
            block-interval block-interval;
        }
        server-timeout seconds;
        supplicant (single | single-secure | multiple);
        supplicant-timeout seconds;
        transmit-period seconds;
    }
    no-mac-table-binding {
        interface interface-names;
        static mac-address;
    }
    radius-options {
        use-vlan-id;
        use-vlan-name;
    }
    static mac-address {
        vlan-assignment vlan-identifier;
    }
}

Hierarchy Level

[edit protocols dot1x]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Configure an authenticator for 802.1X authentication.

The remaining statements are explained separately. See CLI Explorer.

NOTE: You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.

Default
802.1X authentication is disabled.

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

RELATED DOCUMENTATION

| Configuring 802.1X Interface Settings (CLI Procedure) | 390 |
| Specifying RADIUS Server Connections on Switches (CLI Procedure) | 379 |
| Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479 |
authentication (DHCP Local Server)

Syntax

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
    }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**
- Using External AAA Authentication Services with DHCP | 833
authentication (DHCP Relay Agent)

Syntax

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
    }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

**Description**
Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay configuration. Use the statement at the [edit...dhcpv6] hierarchy levels to configure DHCPv6 support.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>dhcp-relay</th>
<th>1665</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using External AAA Authentication Services with DHCP</td>
<td>833</td>
</tr>
</tbody>
</table>
authentication-key-chains

Syntax

```yaml
text
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
text
```

Hierarchy Level

```
[edit security]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos Limited edition for Junos OS Releases 15.1R8, 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, and 17.4R2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the `authentication-key-chains` statement is configured at the `[edit security]` hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the `[edit protocols]` hierarchy level or with the BFD protocol using the `bfd-liveness-detection` statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately. See CLI Explorer.
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols</th>
<th>286</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Configuring BFD Authentication for Securing Static Routes</td>
<td></td>
</tr>
<tr>
<td>Example: Configuring Hitless Authentication Key Rollover for IS-IS</td>
<td></td>
</tr>
</tbody>
</table>
authentication-order

Syntax

authentication-order [method1 method2...];

Hierarchy Level

[edit system]

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

Description
Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.

Default
If you do not include the authentication-order statement, users are verified based on their configured passwords.

Options
One or more of the following authentication methods listed in the order in which they must be tried:

- **password**—Use the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.

- **radius**—Use RADIUS authentication services.

- **tacplus**—Use TACACS+ authentication services.

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

RELATED DOCUMENTATION

Junos OS User Authentication Methods | 209
**authentication-order**

**Syntax**

```
authentication-order [none | password | radius];
```

**Hierarchy Level**

```
[edit access profile profile-name],
[edit system]
```

**Release Information**

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

**Description**

Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending authentication messages.

**Default**

Not enabled

**Options**

- **none**—No authentication for specified subscribers.
- **password**—Password authentication.
- **radius**—RADIUS authentication.

**NOTE:** The [edit access] hierarchy is not available on QFabric systems.

**Required Privilege Level**

- **admin**—To view this statement in the configuration.
- **admin-control**—To add this statement to the configuration.
authentication-order (Access Profile)

Syntax

```
authentication-order [(none | ldap | password | radius | securid)];
```

Hierarchy Level

```
[edit access profile profile-name]
```

Release Information

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

Description

(EX and QFX Series only) Configure the order of authentication, authorization, and accounting (AAA) methods to use while sending authentication messages.

Default

Not enabled

Options

- **none**—No authentication for specified subscribers.
- **password**—Locally configured password in access profile.
- **radius**—RADIUS authentication.
- **securid**—RSA SecurID authentication.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
authentication-order (Authenticator)

Syntax

```
authentication-order [dot1x | mac-radius | captive-portal];
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 15.1R3 for EX Series switches.

Description

Configure the preferred order of authentication methods that the switch will use when attempting to authenticate a client. If multiple authentication methods are configured on a single interface, when one authentication method fails, the switch falls back to another method. You can configure the `authentication-order` statement to specify whether 802.1X authentication or MAC RADIUS authentication must be the first authentication method tried.

By default, the switch attempts to authenticate a client by using 802.1X authentication first. If 802.1X authentication fails because there is no response from the client, and MAC RADIUS authentication is configured on the interface, the switch falls back to MAC RADIUS authentication. If MAC RADIUS fails, and captive portal is configured on the switch, the switch falls back to captive portal.

Configuring MAC RADIUS authentication as the first method can help prevent the fallback timeout period which occurs after an 802.1X authentication attempt is made for a host that does not support 802.1X authentication. If MAC RADIUS authentication is configured as the first authentication method on an interface, then on receiving data from any client on that interface, the switch attempts to authenticate the client by using MAC RADIUS authentication. If MAC RADIUS authentication fails, then the switch falls back to 802.1X authentication. If 802.1X authentication fails, and captive portal is configured on the interface, the switch falls back to captive portal.

802.1X authentication always has the highest priority, even if a client has been authenticated using another method. If the switch receives an EAP packet from a client that has been authenticated using MAC RADIUS authentication, the switch acknowledges the EAP packet and upgrades the authentication using 802.1X authentication credentials. Similarly, if a client has been authenticated through fallback to captive portal, and the switch receives an EAP packet from that client, the switch attempts to authenticate the client by using 802.1X authentication.

The switch attempts authentication using only methods that are configured on the interface. If an authentication method is included in the authentication order, but is not configured on the interface, the switch ignores that method and attempts authentication using the next method in the order that is enabled.
However, if a method is enabled on the interface, but is not included in the authentication order, the switch does not attempt using that method. For example, if captive portal is enabled for an interface, but the authentication order is configured as `[mac-radius dot1x]`, the authentication method for that interface does not fall back to captive portal.

The authentication order can be configured for all interfaces by using the `interface all` option. If the authentication order is configured for an individual interface, and there is also an authentication order configured for all interfaces, then the order for the individual interface is followed. If there is no authentication order configured for an individual interface, and there is an authentication order configured for all interfaces, then the configuration for all interfaces is followed.

Use the following guidelines when configuring the `authentication-order` statement:

- The authentication order must include at least two methods of authentication.
- 802.1X authentication must be one of the methods included in the authentication order.
- If captive portal is included in the authentication order, it must be the last method in the order.
- If `mac-radius-restrict` is configured on an interface, then the authentication order cannot be configured.

The valid combinations for `authentication-order` are as follows:

- `[dot1x mac-radius captive-portal]`
- `[dot1x captive-portal]`
- `[dot1x mac-radius]`
- `[mac-radius dot1x captive-portal]`

Default

If `authentication-order` is not configured, the switch attempts to authenticate the client by using 802.1X authentication first, followed by MAC RADIUS authentication, and then captive portal, as follows:

1. 802.1X authentication—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.

2. MAC RADIUS authentication—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.

3. Captive portal authentication—If captive portal is configured on the interface, the switch attempts to authenticate the end device by using this method after attempting any other configured authentication methods.
Options

captive-portal—Configure captive portal authentication in the order of authentication methods on the interface.

dot1x—Configure 802.1X authentication in the order of authentication methods on the interface.

mac-radius—Configure MAC RADIUS authentication in the order of authentication methods on the interface.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Authentication on Switches | 361
- Configuring Flexible Authentication Order | 506
authentication-profile-name

Syntax

```bash
authentication-profile-name access-profile-name;
```

Hierarchy Level

```bash
[edit protocols dot1x authenticator],
[edit services captive-portal]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Added to [edit services captive-portal] hierarchy in Junos OS Release 10.1 for EX Series switches.

Description

Specify the name of the access profile to be used for 802.1X, MAC RADIUS, or captive portal authentication.

Default

No access profile is specified.

Options

`access-profile-name`—Name of the access profile. The access profile is configured at the [edit access profile] hierarchy level and contains the RADIUS server IP address and other information used for authentication.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 427
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring Captive Portal Authentication (CLI Procedure) | 492
authentication-protocol

Syntax

```
authentication-protocol (eap-md5 | pap);
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface interface-name mac-radius]
```

Release Information

Statement introduced in Junos OS Release 15.1R3 for EX Series switches.
The `eap-peap` was introduced in Junos OS Release 17.2R1 for EX Series switches.

Description

Specify the protocol to be used by a supplicant to provide authentication credentials for MAC RADIUS authentication. The protocols supported for MAC RADIUS authentication are EAP-MD5, which is the default, Protected Extensible Authentication Protocol (EAP-PEAP), and Password Authentication Protocol (PAP).

Default

If `authentication-protocol` is not configured, the EAP-MD5 authentication protocol is used for MAC RADIUS authentication.

Options

- **eap-md5**—Use the EAP-MD5 protocol for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework. EAP-MD5 uses MD5 to hash the username and password. EAP-MD5 provides for a one-way client authentication. The server sends the client a random request for which the client must provide a response containing an encryption of the request and its password for establishing its identity.

- **eap-peap**—Use the EAP-PEAP protocol, also known as Protected EAP or PEAP, for MAC RADIUS authentication. EAP-PEAP is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel. By encapsulating the authentication process in a TLS tunnel, PEAP addresses the vulnerabilities of an EAP like EAP-MD5.

- **pap**—Use the PAP authentication protocol for MAC RADIUS authentication. PAP provides a simple password-based authentication for users to establish their identity by using a two-way handshake. PAP transmits plaintext passwords over the network without encryption. PAP must be configured if the Lightweight Directory Access Protocol (LDAP), which supports only plaintext passwords for client authentication, is used for RADIUS authentication.

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

RELATED DOCUMENTATION

Understanding Authentication on Switches | 361
Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
authentication-server

Syntax

authentication-server [server-addresses];

Hierarchy Level

[edit access profile profile-name radius]

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

Description
Configure the RADIUS server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options
server-addresses—Configure one or more RADIUS server addresses.

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

RELATED DOCUMENTATION

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
show network-access aaa statistics authentication | 2714
authentication-whitelist

Syntax

```bash
authentication-whitelist {
    mac-address {
        interface interface-name;
        vlan-assignment ( vlan-id | vlan-name);
    }
}
```

Hierarchy Level

```
[edit ethernet-switching-options];
[edit switch-options]
```

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches. The [edit switch-options] hierarchy level was introduced in Junos OS Release 13.2X50-D10 for EX Series switches (ELS).

Description

Configure MAC addresses for which RADIUS authentication is to be bypassed.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Example: Setting Up Captive Portal Authentication on an EX Series Switch with ELS Support | 499
- Configuring Captive Portal Authentication (CLI Procedure) | 492
- Configuring Captive Portal Authentication (CLI Procedure) on an EX Series Switch with ELS Support | 497
authorization

Syntax

authorization authorization;

Hierarchy Level

[edit snmp community community-name]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Set the access authorization for SNMP Get, GetBulk, GetNext, and Set requests.

Options
authorization—Access authorization level:

• read-only—Enable Get, GetNext, and GetBulk requests.
• read-write—Enable all requests, including Set requests. You must configure a view to enable Set requests.

NOTE: The read-write option is not supported on the QFX3000 QFabric system.

Default: read-only

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

RELATED DOCUMENTATION

Configuring the SNMP Community String
authorization-time-interval

Syntax

authorization-time-interval minutes;

Hierarchy Level

[edit system tacplus-options]

Release Information
Statement introduced in Junos OS Release 17.4R1.

Description
Configure the time interval at which the JUNOS device has to fetch the authorization profile configuration from the TACACS+ server and refresh the authorization profile stored locally on the JUNOS device. The TACACS+ server sends the authorization profile once by default after the user is successfully authenticated, and the authorization profile is stored locally on the JUNOS device. The authorization profile refresh feature enables the JUNOS device to check the authorization profile configured remotely on the TACACS+ server at the configured time interval.

If there is a change in the remote authorization profile, the device fetches the authorization profile from the TACACS+ server and the authorization profile configured locally under the login class hierarchy. The device refreshes the authorization profile stored locally by combining the remote and locally-configured authorization profiles. This ensures that any changes made to the authorization profile configuration on the TACACS+ server are reflected on the JUNOS device without the user having to restart the authentication process.

To enable periodic refresh of the authorization profile, you must set the time interval at which the JUNOS device has to fetch the authorization profile configuration from the TACACS+ server and refresh the authorization profile stored locally. The time interval can be configured directly on the TACACS+ server or locally on the JUNOS device using the CLI. Use the following guidelines to determine which time interval configuration takes precedence:

- If there is no refresh time interval configured on the TACACS server for periodic refresh, the JUNOS device does not receive the time interval value in the authorization response. In this case, the value configured locally on the JUNOS device will take effect.
- If the refresh time interval is configured on the TACACS server and there is no refresh time interval configured locally on the JUNOS device, the value configured on the TACACS server will take effect.
- If refresh time interval is configured on the TACACS server and also on the JUNOS device locally, the value configured on the TACACS server will take precedence.
• If there is no refresh time interval configured on the TACACS server and there is no refresh time interval configured on the JUNOS device, there will be no periodic refresh.

• If the refresh time interval configured on the TACACS server is out of range or invalid, the refresh time interval value configured locally will take effect.

• If the refresh time interval configured on the TACACS server is out of range or invalid and there is no refresh time interval configured locally, there will be no periodic refresh.

After the periodic refresh time interval is set, if the user changes the refresh interval before the authorization request is sent from the JUNOS device, the updated refresh interval takes effect after the next immediate periodic refresh.

**Default**
If the authorization time interval is not configured, the authorization profile is not refreshed during a TACACS+ authentication session.

**Options**

*minutes*—The time interval at which the authorization profile that is configured on the TACACS+ server is fetched by the JUNOS device during a TACACS+ authentication session.

**Range:** 15 to 1440 minutes.

**Required Privilege Level**

admin—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

| tacplus-options | 2308 |
| Configuring Periodic Refresh of the TACACS+ Authorization Profile | 271 |
backoff-factor

Syntax

backoff-factor seconds;

Hierarchy Level

[edit system login retry-options]

Release Information
Statement introduced in Junos OS Release 8.0.

Description
Configure the length of delay after each failed login attempt, which increases for each subsequent login attempt after the value specified in the backoff-threshold statement.

Options

seconds—Length of delay after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold option.

Range: 5 through 10
Default: 5

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

RELATED DOCUMENTATION

Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82
retry-options | 2205
backoff-threshold

Syntax

backoff-threshold number;

Hierarchy Level

[edit system login retry-options]

Release Information
Statement introduced in Junos OS Release 8.0.

Description
Configure the threshold for the number of failed login attempts on the router before the user experiences a delay when attempting to reenter a password.

Options

number—Threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Use the backoff-factor option to specify the length of delay, in seconds.

Range: 1 through 3
Default: 2

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

RELATED DOCUMENTATION

Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82
retry-options | 2205
backup-on-failure (Accounting Options)

Syntax

```
backup-on-failure (master-and-slave | master-only);
```

Hierarchy Level

[edit accounting-options file filename]

Release Information


Description

Configure the router to save a copy of the accounting file locally, to the /var/log/pfedBackup directory of the relevant Routing Engine, in the event that file transfer to the remote archive sites cannot be completed.

Options

- **master-and-slave**—Back up accounting files from both the master Routing Engine and the backup Routing Engine.

- **master-only**—Back up accounting files from only the master Routing Engine.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Accounting-Data Log Files
- Configuring Flat-File Accounting for Layer 2 Wholesale
- Configuring Flat-File Accounting for Extensible Subscriber Services Management
- Flat-File Accounting Overview
**bfd**

**Syntax**

```
bfd {
version (0 | 1 | automatic);
minimum-interval milliseconds;
minimum-receive-interval milliseconds;
multiplier number;
no-adaptation;
transmit-interval {
  minimum-interval milliseconds;
  threshold milliseconds;
}
detection-time {
  threshold milliseconds;
}
session-mode (automatic | multihop | singlehop);
holddown-interval milliseconds;
}
```

**Hierarchy Level**

- [edit system services dhcp-local-server liveness-detection method]
- [edit system services dhcp-local-server dhcpv6 liveness-detection method]
- [edit forwarding-options dhcp-relay liveness-detection method]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
- [edit system services dhcp-local-server group group-name liveness-detection method]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
- [edit forwarding-options dhcp-relay group group-name liveness-detection method]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

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

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
**block-interval**

**Syntax**

```
block-interval block-interval;
```

**Hierarchy Level**

```
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan (vlan-id | vlan-name)],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan]
```

**Release Information**

Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**

Specify the amount of time that the 802.1X interface ignores Extensible Authentication Protocol (EAP) start messages from the client when an EAPoL block has been enabled on the 802.1X interface.

**Options**

- **block-interval**—The number of seconds for the interval.

**Range:** 120 through 65,535

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- [eapol-block][1] | 1752
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients | 415
boot-loader-authentication

Syntax

```plaintext
boot-loader-authentication {
  (encrypted-password password | plain-text-password);
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description

Set the boot-loader password for accessing the U-Boot CLI during the boot process. The password can be entered either as a plain-text password or as an encrypted password.

Encrypted passwords must be entered in Message Digest 5 (MD5) format. Plain-text passwords are encrypted by using MD5 by default. The encryption format for plain-text passwords can be changed by using the `set system login password format` command.

Encrypted passwords must be between 1 and 128 characters long. The password must be enclosed in quotation marks and cannot be blank within the quotation marks (" ").

The default requirements for plain-text passwords are as follows:

- The password must be between 6 and 128 characters long
- You can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters). Control characters are not recommended.
- The password must contain at least one change of case or character class.

Options

`encrypted-password password`—Enter a password that has already been encrypted. You can specify only one encrypted password.

`plain-text-password`—Enter a plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

Required Privilege Level

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

RELATED DOCUMENTATION

| Using Unattended Mode for U-Boot to Prevent Unauthorized Access | 375 |
| format | 1802 |
| unattended-boot | 2381 |
boot-server (NTP)

Syntax

```
boot-server (address | hostname);
```

Hierarchy Level

```
[edit system ntp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the server that NTP queries when the SRX Series device boots to determine the local date and time.

When you boot the SRX Series device, it issues an `ntpdate` request, which polls a network server to determine the local date and time. You need to configure a server that the SRX Series device uses to determine the time when the SRX Series device boots. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the `ntpdate` request resolves the hostname to an IP address when the SRX Series device boots up.

If you configure an NTP boot server, then when the SRX Series device boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.

Options

- `address`—The IP address of an NTP boot server.
- `hostname`—The hostname of an NTP boot server.

Required Privilege Level

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

RELATED DOCUMENTATION

```
ntp | 2005
```
boot-server (NTP)

Syntax

```plaintext
boot-server (address | hostname);
```

Hierarchy Level

```
[edit system ntp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

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

When you boot the router, switch, or SRX Series device, it issues an `ntpdate` request, which polls a network server to determine the local date and time. You need to configure a server that the router, switch, or SRX Series device uses to determine the time when the device boots. Otherwise, NTP cannot synchronize to a time server if the server time significantly differs from the local device's time. You can configure either an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the `ntpdate` request resolves the hostname to an IP address when the router, switch, or SRX Series device boots up.

If you configure an NTP boot server, then when the SRX Series device boots, it immediately synchronizes with the boot server even if the NTP process is explicitly disabled or if the time difference between the client and the boot server exceeds the threshold value of 1000 seconds.

Options

- `address`—IP address of an NTP boot server.
- `hostname`—Hostname of an NTP boot server.

Required Privilege Level

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

RELATED DOCUMENTATION
### boot-server (DHCP)

**Syntax**

```
boot-server (address | hostname);
```

**Hierarchy Level**

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

**Release Information**

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

**Description**

Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.

**Options**

- `address`—IP address of a DHCP boot server.
- `hostname`—Hostname of a DHCP boot server.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- `boot-file`
**broadcast**

**Syntax**

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

**Hierarchy Level**

```
[edit system ntp]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

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

**Options**

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

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

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

  **Default:** The default routing instance is used to broadcast packets.

- **routing-instance-name routing-instance-name**—(Optional) The routing instance name in which the interface has an address in the broadcast subnet.

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

  **Range:** 1 through 255

  **Default:** 1

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

  **Range:** 1 through 4

  **Default:** 4

**Required Privilege Level**

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

ntp | 2005
broadcast

Syntax

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

Hierarchy Level

- [edit system ntp]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

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

Options

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

- **key key-number**—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number (any unsigned 32-bit integer).

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

  Range: 1 through 255

  Default: 1

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

  Range: 1 through 4

  Default: 4

Required Privilege Level

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

RELATED DOCUMENTATION

- **Understanding NTP Time Servers**
broadcast-client

Syntax

```
broadcast-client;
```

Hierarchy Level

```
[edit system ntp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the SRX Series device to listen for broadcast messages on the local network to discover other servers on the same subnet.

Required Privilege Level

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

RELATED DOCUMENTATION

- ntp | 2005
**broadcast-client**

**Syntax**

```
broadcast-client;
```

**Hierarchy Level**

```
[edit system ntp]
```

**Release Information**

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

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

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Understanding NTP Time Servers*
- *Configuring NTP Authentication Keys*
- *Configuring the Switch to Listen for Broadcast Messages Using NTP*
ca-name

Syntax

ca-name ca-identity;

Hierarchy Level

[edit security certificates certification-authority]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

Options
ca-identity—CA identity to use in the certificate request.

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

RELATED DOCUMENTATION

Specifying the Certificate Authority Name
ca-type

Syntax

```plaintext
ca-type {
  number {
    ca-value value;
  }
}
```

Hierarchy Level

[edit protocols lldp-med interface (all | interface-name location civic-based)]

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the address elements. These elements are included in the location information to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

For further information about the values that can be used to comprise the location, refer to RFC 4776, *Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information*. A subset of those values is provided below.

The `ca-value` statement is explained separately.

Default

Disabled.

Options

`value`—Civic address elements that represent the civic or postal address. Values are:

- `0`—A code that specifies the language used to describe the location.
- `16`—The leading-street direction, such as "N".
- `17`—A trailing street suffix, such as "SW".
- `18`—A street suffix or type, such as "Ave" or "Platz".
- `19`—A house number, such as "6450".
- `20`—A house-number suffix, such as "A" or "1/2".
- `21`—A landmark, such as "Stanford University".
• 22—Additional location information, such as "South Wing".
• 23—The name and occupant of a location, such as "Carrillo’s Holiday Market".
• 24—A house-number suffix, such as "95684".
• 25—A building structure, such as “East Library”.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>show lldp</th>
<th>2680</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</td>
<td>528</td>
</tr>
<tr>
<td>Configuring LLDP-MED (CLI Procedure)</td>
<td>665</td>
</tr>
</tbody>
</table>
ca-value

Syntax

ca-value value;

Hierarchy Level

[edit protocols lldp-med interface (all | interface-name) location civic-based ca-type number]

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

Description
For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure location information, such as street address and city, that is indexed by the ca-type code. This information is advertised from the switch to the MED and is used during emergency calls to identify the location of the MED.

Default
Disabled.

Options
value—Specify a value that correlates to the ca-type. See ca-type for a list of codes and suggested values.

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

RELATED DOCUMENTATION

| show lldp | 2680 |
| Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528 |
| Configuring LLDP-MED (CLI Procedure) | 665 |
cache-size

Syntax

cache-size bytes;

Hierarchy Level

[edit security certificates]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.

Options
bytes—Cache size for digital certificates.

Range: 64 through 4,294,967,295
Default: 2 megabytes (MB)

NOTE: We recommend that you limit your cache size to 4 MB.

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

RELATED DOCUMENTATION

Configuring the Cache Size
cache-timeout-negative

Syntax

```
cache-timeout-negative seconds;
```

Hierarchy Level

```
[edit security certificates]
```

Release Information

Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.

Options

seconds—Negative time to cache digital certificates, in seconds.

Range: 10 through 4,294,967,295  
Default: 20

CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Negative Cache
captive-portal

Syntax

captive-portal {
  authentication-profile-name authentication-profile-name
  custom-options {
    banner-message string;
    footer-bgcolor color;
    footer-message string;
    footer-text-color color;
    form-header-bgcolor color;
    form-header-message string;
    form-header-text-color color;
    form-reset-label label-name;
    form-submit-label label-name;
    header-bgcolor color;
    header-logo filename;
    header-message string;
    header-text-color color;
    post-authentication-url url-string;
  }
  interface (all | [interface-names]) {
    quiet-period seconds;
    retries number-of-retries;
    server-timeout seconds;
    session-expiry seconds;
    supplicant (multiple | single | single-secure);
  }
  secure-authentication (http | https);
}

Hierarchy Level

[edit services]

Release Information
Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description
Configure captive portal to authenticate clients connected to the switch for access to the network.

The remaining statements are explained separately. See CLI Explorer.
Default
Captive portal is disabled.

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

RELATED DOCUMENTATION

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Designing a Captive Portal Authentication Login Page on Switches | 494
Configuring Captive Portal Authentication (CLI Procedure) | 492
Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
certificate-verification

Syntax

```
certificate-verification (optional | required | warning);
```

Hierarchy Level

```
[edit services unified-access-control]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Specify certificate verification requirement for the connection from the switch to Junos Pulse Access Control service.

Default

warning

Options

optional—The specification of a security certificate is optional.
required—The specification of a security certificate is required.

NOTE: Do not specify this option in Junos OS Release 12.2 for EX Series switches, because the specification of a security certificate (ca-profile) is not supported in this release.

warning—A warning is issued if a security certificate is not specified. Default.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
certificates

Syntax

certificates {
cache-size bytes;
cache-timeout-negative seconds;
certification-authority ca-profile-name {
  ca-name ca-identity;
crl file-name;
  encoding (binary | pem);
enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
enrollment-retry attempts;
local certificate-name {
  certificate-key-string;
  load-key-file URL filename;
}
  maximum-certificates number;
  path-length certificate-path-length;
}

Hierarchy Level

[edit security]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificates for IPsec.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.
RELATED DOCUMENTATION

Configuring Digital Certificates for an ES PIC
certification-authority

Syntax

certification-authority ca-profile-name {
  ca-name ca-identity;
  crl file-name;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}

Hierarchy Level

[edit security certificates]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced before Junos OS Release 12.1 for the SRX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

Configure certification authority (CA) for X.509 certificate.

Options
• profile-name—Name of this CA configuration.
• ca-name name—Name of the CA.
• crl filename—Certificate revocation list (CRL) filename.
• encoding—Certificate encoding, either binary or pem (privacy-enhanced mail).
• enrollment-url url—Enrollment URL.
• file filename—Certificate filename.
• ldap-url url—Lightweight Directory Access Protocol (LDAP) URL.

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

RELATED DOCUMENTATION

- Configuring the Certificate Authority Properties for an ES PIC
- Configuring the Certificate Authority Properties for an ES PIC
change-type

Syntax

```
change-type (character-sets | set-transitions);
```

Hierarchy Level

```
[edit system login password]
```

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

Description
Set requirements for using character sets in plain-text passwords. When you combine this statement with the `minimum-changes` statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements.

Options
Specify one of the following:

- `character-sets`—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.
- `set-transitions`—The number of transitions between character sets.

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

RELATED DOCUMENTATION

```
minimum-changes | 1953
```
civic-based

Syntax

civic-based { 
    what number; 
    country-code code; 
    ca-type { 
        number { 
            ca-value value; 
        } 
    } 
} 

Hierarchy Level

[edit protocols lldp-med interface (all | interface-name) location]

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

Description
For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the geographic location to be advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

The remaining statements are explained separately. See CLI Explorer.

Default
Disabled.

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

RELATED DOCUMENTATION

| show lldp | 2680 |
| Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528 |
| Configuring LLDP-MED (CLI Procedure) | 665 |
ciphers

Syntax

ciphers [ cipher-1 cipher-2 cipher-3 ...]

Hierarchy Level

[edit system services ssh]

Release Information
Statement introduced in Junos OS Release 11.2.

Description
Specify the set of ciphers the SSH server can use to perform encryption and decryption functions.

Options
- **3des-cbc**—Triple Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
- **aes128-cbc**—128-bit Advanced Encryption Standard (AES) in CBC mode.
- **aes128-ctr**—128-bit AES in counter mode.
- **aes128-gcm@openssh.com**—128-bit AES in Galois/Counter Mode.
- **aes192-cbc**—192-bit AES in CBC mode.
- **aes192-ctr**—192-bit AES in counter mode.
- **aes256-cbc**—256-bit AES in CBC mode.
- **aes256-ctr**—256-bit AES in counter mode.
- **aes256-gcm@openssh.com**—256-bit AES in Galois/Counter Mode.
- **arcfour**—128-bit RC4-stream cipher in CBC mode.
- **arcfour128**—128-bit RC4-stream cipher in CBC mode.
- **arcfour256**—256-bit RC4-stream cipher in CBC mode.
- **blowfish-cbc**—128-bit blowfish-symmetric block cipher in CBC mode.
- **cast128-cbc**—128-bit cast in CBC mode.
- **chacha20-poly1305@openssh.com**—ChaCha20 stream cipher and Poly1305 MAC
NOTE: Ciphers represent a set. To configure SSH ciphers use the `set` command as shown in the following example:

```
user@host#set system services ssh ciphers [ aes256-cbc aes192-cbc ]
```

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

**RELATED DOCUMENTATION**

- Configuring SSH Service for Remote Access to the Router or Switch | 294
- key-exchange | 1890
- macs | 1933
circuit-id (DHCP Relay Agent)

Syntax

circuit-id {
    include-irb-and-l2;
    keep-incoming-circuit-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
}

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Specify the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix, textual description, or VLAN tag.

NOTE: For Layer 3 interfaces, when you configure relay-option-82 only, the Agent Circuit ID is the default. If no VLAN tags are configured, then the default is the logical interface device (IFL) name. For integrated routing and bridging (IRB) interfaces, the default is the Layer 2 IFL name and bridge domain name.
The interface to bridge domain relationship may be implicit (the interface is mapped to the bridge domain by the system based on VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs), stacked VLANs (S-VLANs), or bridge domains is as follows:

(fe | ge)-fpc/pic/port.subunit

**NOTE:** For remote systems, the *subunit* is required and is used to differentiate an interface for remote systems.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

(fe | ge)-fpc/pic/port:vlan-id

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

(fe | ge)-fpc/pic/port:svlan-id-vlan-id

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-fpc/pic/port:subunit:bridge-domain-name

- IRB interfaces that use VLANs:

  (fe | ge)-fpc/pic/port:subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the `include-irb-and-l2` statement. The format is as follows:
• IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

• IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the no-vlan-interface-name statement. The format is as follows:

irb.subunit

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Using DHCP Relay Agent Option 82 Information | 739
- Configuring Option 82 Information
circuit-type

Syntax

circuit-type;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]

Release Information
Statement introduced in Junos OS Release 9.1.

Description
Specify that the circuit type is concatenated with the username during the subscriber authentication process.

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

RELATED DOCUMENTATION

Using External AAA Authentication Services to Authenticate DHCP Clients | 728
circuit-type (DHCP Local Server)

Syntax

circuit-type;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.

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

**RELATED DOCUMENTATION**
- Using External AAA Authentication Services with DHCP | 833
circuit-type (DHCP Relay Agent)

Syntax

circuit-type;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description

Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Required Privilege Level

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

RELATED DOCUMENTATION

Using External AAA Authentication Services with DHCP | 833
Creating Unique Usernames for DHCP Clients | 834
class (Defining Login Classes)

Syntax

class class-name {
    access-end hh:mm;
    access-start hh:mm;
    ( allow-commands "(regular-expression1)|(regular-expression2)...") allow-commands-regexps ["regular expression 1" "regular expression 2" ... ]);
    ( allow-configuration "(regular-expression1)|(regular-expression2)...") allow-configuration-regexps ["regular expression 1" "regular expression 2" ... ]);
    allow-hidden-commands;
    allow-sources [ allow-sources ... ];
    allow-times [ allow-times ... ];
    allowed-days [ days of the week ];
    cli {
        prompt prompt;
    }
    configuration-breadcrumbs;
    confirm-commands ["regular expression or command 1" "regular expression or command 2" ...] {
        confirmation-message;
    }
    ( deny-commands "(regular-expression1)|(regular-expression2)...") deny-commands-regexps ["regular expression 1" "regular expression 2" ... ]);
    ( deny-configuration "(regular-expression1)|(regular-expression2)...") deny-configuration-regexps ["regular expression 1" "regular expression 2" ... ]);
    deny-sources [ deny-sources ... ];
    deny-times [ deny-times ... ];
    idle-timeout minutes;
    logical-system logical-system-name;
    login-alarms;
    login-script login-script;
    login-tip;
    no-hidden-commands {
        except ["regular expression or command 1" "regular expression or command 2" ... ];
    }
    no-scp-server;
    no-sftp-server;
    permissions [ permissions ];
    satellite all;
    security-role (audit-administrator | crypto-administrator | ids-administrator | security-administrator);
    tenant tenant-system-name;
}
Hierarchy Level

[edit system login]

Release Information
The class, allow-commands, deny-commands, allow-configuration, deny-configuration, idle-timeout, login-alarms, login-tip, and permissions statements were introduced before Junos OS Release 7.4.
All of the previously mentioned statements were introduced in Junos OS Release 9.0 for the EX Series.
The login-script statement was introduced in Junos OS Release 9.5.
The access-end, access-start, and allowed-days statements were introduced in Junos OS Release 10.1.
All of the previously mentioned statements were introduced in Junos OS Release 11.1 for the QFX Series.
All of the previously mentioned statements were introduced in Junos OS Release 11.2 for the SRX Series.
The allow-configuration-regexp, deny-configuration-regexp, and security-role statements were introduced in Junos OS Release 11.2.
The configuration-breadcrumbs statement was introduced in Junos OS Release 12.2.
All of the previously mentioned statements were introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
All of the previously mentioned statements were introduced in Junos OS Release 15.1X49-D70 for the vSRX, SRX4100, SRX4200 and SRX1500 devices.
All of the previously mentioned statements were introduced in Junos OS Release 16.1 for the MX Series and PTX Series.
The allow-hidden-commands, confirm-commands, no-hidden-commands, and satellite statements were introduced in Junos OS Release 16.1.
The cli statement was introduced in Junos OS Release 17.3.
The allow-commands-regexp and deny-commands-regexp statements were introduced in Junos OS Release 18.1.
The tenant statement was introduced in Junos OS 18.4.
The no-scp-server and no-sftp-server statements were introduced in Junos OS Release 19.2.

Description
Define a login class. All users who log in to the router or switch must be in a login class. Therefore, you must define a Junos OS login class for each user or type of user. You can define any number of login classes depending on the types of permissions the users need. You may not need to define any login classes; Junos OS has several predefined login classes, to suit a variety of needs. However, the predefined login classes cannot be modified. If you define a class with the same name as a predefined class, Junos OS appends -local to the login class name and creates a new login class. See "Predefined System Login Classes" on page 69 for more information.
Options

**class-name**— A name you choose for the login class.

**access-end**— Specify the end time in **HH:MM** (24-hour) format, where **HH** represents the hours and **MM** represents the minutes.

| NOTE: Access start and end times that span across 12:00 AM starting on a specified day results in the user having access until the next day, even if the access day is not explicitly configured on the **allowed-days** statement. |

**access-start**— Specify the start time in **HH:MM** (24-hour) format, where **HH** represents the hours and **MM** represents the minutes.

| NOTE: Access start and end times that span across 12:00 AM starting on a specified day results in the user having access until the next day, even if the access day is not explicitly configured on the **allowed-days** statement. |

**( allow-commands | allow-commands-regexps )**— Specify one or more regular expressions to allow users in this class to issue operational mode commands. You use the **allow-commands** or the **allow-commands-regexps** statement to explicitly allow authorization for commands that would otherwise be denied by the access privilege levels for a login class.

For the **allow-commands** statement, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

For the **allow-commands-regexps** statement, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the **allow-command** statement. You can also include values for variables in the regular expressions, which is not supported using the **allow-commands** statement.

The **deny-commands** or the **deny-commands-regexps** statement takes precedence if it is used in the same login class definition.

| NOTE: The **allow/deny-commands** and **allow/deny-commands-regexps** statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the **allow/deny-commands** statements, or the **
allow/deny-commands-regexps statements. If you have existing configurations using the allow/deny-commands statements, using the same configuration options with the allow/deny-commands-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific TACACS+ attributes in your authentication server's configuration. For a remote user, when the authorization parameters are configured both remotely and locally, authorization parameters configured remotely and locally are both considered together for authorization. For a local user, only the authorization parameters configured locally for the class are considered.

**Default:** If you do not configure authorizations for operational mode commands using the allow/deny-commands or allow/deny-commands-regexps statements, users can edit only those commands for which they have access privileges set with the permissions statement.

**Syntax:** regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.
(allow-configuration | allow-configuration-regexps)—Specify one or more regular expressions to explicitly allow users in this class to access the specified levels in the configuration hierarchy even if the permissions set with the permissions statement do not grant such access.

For the allow-configuration statement, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses ( ). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

For the allow-configuration-regexps statement, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the allow/deny-configuration statements. You can also include values for variables in the regular expressions, which is not supported using the allow/deny-configuration statements.

The deny-configuration or deny-configuration-regexps statement takes precedence if it is used in the same login class definition.

NOTE: The allow/deny-configuration and allow/deny-configuration-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-configuration statements, or the allow/deny-configuration-regexps statements. If you have existing configurations using the allow/deny-configuration statements, using the same configuration options with the allow/deny-configuration-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default: If you omit the allow-configuration/allow-configuration-regexps statement and the deny-configuration/deny-configuration-regexps statement, users can edit only those commands for which they have access privileges through the permissions statement.

Syntax: regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.

allow-hidden-commands—Allow all hidden commands to be run. If the no-hidden-commands statement is specified at the [edit system] hierarchy level, overrides that restriction for this login class. Hidden commands are Junos OS commands that are not published but could be run on a router. Hidden commands serve a specific purpose, but for most part are not expected to be used, and as such are not actively supported. The no-hidden-commands statement at the [edit system] hierarchy level allows you to block all hidden commands to all users except the root users.

Default: Hidden commands are enabled by default.
allow-sources [ allow-sources ...]— Restrict incoming remote access to certain hosts.

allow-times [ allow-times... ]— Restrict remote access to certain times.

allowed-days [ days of the week ]— Specify one or more days of the week when users in this class are allowed to log in.

Values:

- monday—Monday
- tuesday—Tuesday
- wednesday—Wednesday
- thursday—Thursday
- friday—Friday
- saturday—Saturday
- sunday—Sunday

cli— Set the CLI prompt specified for the login class. If a CLI prompt is also set at the [edit system login user cli] hierarchy level, the prompt set for the login user has precedence over the prompt set for the login class.

prompt prompt— Specify the prompt string you want to see displayed in the CLI prompt.

configuration-breadcrumbs— Enable the configuration breadcrumbs view in the CLI to display the location in the configuration hierarchy. For an example of how to enable this view, see Example: Enabling Configuration Breadcrumbs.

confirm-commands— Specify that confirmation for particular commands is explicitly required and, optionally, specify the wording of the message displayed at confirm time. You can specify the commands using a list of regular expressions or commands.

Syntax: message

Default: If you omit this option, then confirmation for commands is not required. If the optional message is not set, then the default "Do you want to continue?" message is displayed.
(deny-commands | deny-commands-regexps)—Specify one or more regular expressions to explicitly deny users in this class permission to issue operational mode commands, even though the permissions set with the permissions statement would allow it.

For the deny-commands statement, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

For the deny-commands-regexps statement, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the allow/deny-command statements. You can also include values for variables in the regular expressions, which is not supported using the allow/deny-commands statements.

Expressions configured with the deny-commands or the deny-commands-regexps statement take precedence over expressions configured with allow-commands/allow-commands-regexps if the two statements are used in the same login class definition.

NOTE: The allow/deny-commands and allow/deny-commands-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-commands statements, or the allow/deny-commands-regexps statements. If you have existing configurations using the allow/deny-commands statements, using the same configuration options with the allow/deny-commands-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Authorizations can also be configured remotely by specifying Juniper Networks vendor-specific TACACS+ attributes in your authentication server’s configuration. For a remote user, when the authorization parameters are configured both remotely and locally, authorization parameters configured remotely and locally are both considered together for authorization. For a local user, only the authorization parameters configured locally for the class are considered.

Default: If you do not configure authorizations for operational mode commands using allow/deny-commands or allow/deny-commands-regexps, users can edit only those commands for which they have access privileges set with the permissions statement.

Syntax: regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.
(deny-configuration | deny-configuration-regexps)—Specify one or more regular expressions to explicitly deny users in this class access to the specified levels in the configuration hierarchy even if the permissions set with the permissions statement grant such access. Note that the user cannot view a particular hierarchy if configuration access is denied for that hierarchy.

For the deny-configuration statement, each expression separated by a pipe (|) symbol must be a complete standalone expression, and must be enclosed in parentheses (). Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

For the deny-configuration-regexps statement, you configure a set of strings in which each string is a regular expression, enclosed in double quotes and separated with a space operator. Each string is evaluated against the full path of the command, which provides faster matching than the allow/deny-configuration statements. You can also include values for variables in the regular expressions, which is not supported using the allow/deny-configuration statements.

Expressions configured with deny-configuration/deny-configuration-regexps take precedence over expressions configured with allow-configuration/allow-configuration-regexps if the two statements are used in the same login class definition.

NOTE: The allow/deny-configuration and allow/deny-configuration-regexps statements are mutually exclusive and cannot be configured together for a login class. At a given point in time, a login class can include either the allow/deny-configuration statements, or the allow/deny-configuration-regexps statements. If you have existing configurations using the allow/deny-configuration statements, using the same configuration options with the allow/deny-configuration-regexps statements might not produce the same results, as the search and match methods differ in the two forms of these statements.

Default: If you omit the deny-configuration/deny-configuration-regexps statement and the allow-configuration/allow-configuration-regexps statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the permissions statement.

Syntax: regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. Enter as many expressions as needed.
deny-sources—Never allow remote access from these hosts.

deny-times—Never allow remote access during these times.

idle-timeout—For a login class, configure the maximum time in minutes that a session can be idle before the session times out and the user is logged out of the device. The session times out after remaining at the CLI operational mode prompt for the specified time.

NOTE: After the user logs in to a device from a shell prompt such as csh, if the user starts another program to run in the foreground of the CLI, the idle-timer control is stopped from being computed. The calculation of the idle time of the CLI session is restarted only after the foreground process exits and the control is returned to the shell prompt. When the restart of the idle-timer control occurs, if no interaction from the user occurs on the shell, the user is automatically logged out after the time set on this statement.

Default: If you omit this statement, a user is never forced off the system after extended idle times.
Syntax: minutes—Maximum time in minutes that a session can be idle before a user is logged out.
Range: Range: 0 through 4294967295 minutes

NOTE: The idle-timeout feature is disabled if the value of minutes is set to 0.

login-alarms—Display system alarms when a user with admin permissions logs in to the device. For more information about configuring this statement, see “Configuring System Alarms to Appear Automatically Upon Login” on page 78.

login-script—Run the specified op script when a user belonging to the class logs in to the CLI. The script must be enabled in the configuration.

logical-system—Assign the users in this login class to a logical system. If you specify a logical system, you can't include the satellite configuration statement in the configuration for this login class.

login-tip—Display CLI tips when logging in.
Default: If this statement is not configured, CLI tips are not displayed.

no-hidden-commands—Deny all hidden commands, except for those specified, for users in this login class. Each command listed as an exception must be enclosed in quotation marks.
Default: Hidden commands are enabled by default.
Syntax: except ["command 1" "command 2"...]
no-scp-server— Disable incoming SCP connections for this login class.

no-sftp-server— Disable incoming SFTP connections for this login class.

permissions— Specify login access privileges for the login class.

Syntax: permissions— One or more permission flags, which together specify the access privileges for the login class. Permission flags are not cumulative, so for each class, you must list all the permission flags needed, including view to display information and configure to enter configuration mode. For a list of permission flags, see “Login Class Permission Flags” on page 119.

satellite— Specify access to Junos Fusion satellite devices for the login class. All users assigned to the login class are satellite users. If you include this statement, you can’t include the logical-system configuration statement in the configuration for this login class.

Values:

- all—Specify all Junos Fusion satellite devices.

security-role— Specify one or more Common Criteria (ISO/IEC 15408) security roles for the login class.

Values:

audit-administrator— Specify which users are responsible for the regular review of specific target of evaluation (TOE) audit data and audit trail deletion. Audit administrators can also invoke the non-cryptographic self-test.

crypto-administrator— Specify which users are responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE audit data.

ids-administrator— Specify which users can act as intrusion detection service (IDS) administrators, who are responsible for all of the activities regarding identity and access management of the organization’s employees.

security-administrator— Specify which users are responsible for ensuring that the organization’s security policy is in place.

tenant— Assign the users in this class to a tenant system. Tenant systems are used when you need to separate departments, organizations, or customers and each of them can be limited to one virtual router. The main difference between a logical system and a tenant system is that a logical system supports advanced routing functionality using multiple routing instances. In comparison, a tenant system supports only one routing instance, but supports the deployment of significantly more tenants per system.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.
## RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining Junos OS Login Classes</td>
<td>73</td>
</tr>
<tr>
<td>Configuring Time-Based User Access</td>
<td></td>
</tr>
<tr>
<td>Understanding Junos OS Access Privilege Levels</td>
<td>118</td>
</tr>
<tr>
<td>Example: Configuring User Permissions with Access Privileges for Operational Mode Commands</td>
<td>145</td>
</tr>
<tr>
<td>Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies</td>
<td>128</td>
</tr>
<tr>
<td>Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies</td>
<td>160</td>
</tr>
<tr>
<td>Example: Configuring User Permissions with Access Privilege Levels</td>
<td>124</td>
</tr>
<tr>
<td>Configuring System Alarms to Appear Automatically Upon Login</td>
<td>78</td>
</tr>
<tr>
<td>Executing an Op Script</td>
<td></td>
</tr>
<tr>
<td>Understanding Administrative Roles</td>
<td>106</td>
</tr>
<tr>
<td>Example: Configuring Administrative Roles</td>
<td>108</td>
</tr>
<tr>
<td>Tenant Systems Overview</td>
<td></td>
</tr>
</tbody>
</table>

**user** | 2402
class-usage-profile

Syntax

```plaintext
class-usage-profile profile-name {
    file filename;
    interval minutes;
    source-classes {
        source-class-name;
    }
    destination-classes {
        destination-class-name;
    }
}
```

Hierarchy Level

[edit accounting-options]

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

Description
Create a class usage profile, which is used to log class usage statistics to a file in the /var/log directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has destination-class-usage configured.

For information about configuring source classes, see the Junos Routing Protocols Configuration Guide. For information about configuring source class usage, see the Junos Network Management Configuration Guide.

Options

- `profile-name`—Name of the destination class profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION
configuration-key (DHCP Local Server)

Syntax

```plaintext
configuration-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
}
```

Hierarchy Level

```plaintext
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name ]
```

Release Information

Statement introduced in Junos OS Release 17.3.

Description

Different mechanisms to identify a single household.

Options

- circuit-id—Circuit-id as key.
- mac-address—MAC address of client.
- remote-id—Remote-id as key.

Required Privilege Level

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

RELATED DOCUMENTATION

- Single-Session DHCP Dual-Stack Overview
classification-key (DHCP Relay Agent)

Syntax

classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
}

Hierarchy Level

[edit bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit logical-systems name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit logical-systems name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
Release Information
Statement introduced in Junos OS Release 17.3.

Description
Different mechanisms to identify a single household.

Options
- circuit-id—Circuit-id as key
- mac-address—MAC address of client
- remote-id—Remote-id as key

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

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview
clear-on-abort (DHCP Local Server)

Syntax

```
clear-on-abort;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description

Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

Default

Restores the original client configuration when reconfiguration fails.
Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails | 848
client-alive-count-max

Syntax

```
client-alive-count-max number;
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information

Statement introduced in Junos OS Release 11.2.

Description

Configure the number of client alive messages that can be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. Client alive messages are sent through the encrypted channel. Use in conjunction with client-alive-interval to disconnect unresponsive SSH clients.

Default

3 messages

Options

Range: 0 through 255

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Configuring SSH Service for Remote Access to the Router or Switch | 294
client-alive-interval

Syntax

client-alive-interval seconds;

Hierarchy Level

[edit system services ssh]

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Configure a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. This option applies to SSH protocol version 2 only. Use in conjunction with client-alive-count-max to disconnect unresponsive SSH clients.

Default

0 seconds

Options

Range: 1 through 65535

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Configuring SSH Service for Remote Access to the Router or Switch | 294 |
client-discover-match (DHCP Local Server)

Syntax

client-discover-match <option60-and-option82 | incoming-interface>;

Hierarchy Level

[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server group group-name interface interface-name overrides]
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ... overrides],
[edit logical-systems logical-system-name system services dhcp-local-server ... overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server ... overrides]

Release Information

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
incoming-interface option added in Junos OS Release 13.3.

Description

Configure the match criteria DHCP local server uses to uniquely identify DHCP subscribers or clients when primary identification fails. The options are mutually exclusive.

Default

By default, DHCP uses the option60-and-option82 option.

Options

incoming-interface—(Optional) Allow only one client device to connect on the interface. If the client device changes, the router deletes the existing client binding and creates a binding for the newly connected device.

NOTE: The overrides client-discover-match incoming-interface configuration deletes and replaces the existing binding when a new device connects. This action differs from the overrides interface-client-limit 1 statement, which retains the existing binding and rejects the newly connected client.

option60-and-option82—(Optional) Use option 60 and option 82 information to identify subscribers.
**Required Privilege Level**

*system*—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- Extended DHCP Local Server Overview | 718
- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
- DHCP Auto Logout Overview | 822
- *Allowing Only One DHCP Client Per Interface*
client-ia-type

Syntax

```plaintext
client-ia-type {
   ia-na;
   ia-pd;
}
```

Hierarchy Level

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

Description

Configure the DHCPv6 client identity association type.

Options

- `ia-na`—Identity association for nontemporary address
- `ia-pd`—Identity association for prefix delegation

Required Privilege Level

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

RELATED DOCUMENTATION

- [DHCPv6 Client Overview](#) | 998
client-id (DHCP Local Server)

Syntax

```plaintext
client-id;
```

Hierarchy Level

```plaintext
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the
username during the subscriber authentication or client authentication process.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients | 834
client-id (DHCP Relay Agent)

Syntax

client-id;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the client ID is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

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

RELATED DOCUMENTATION

| Using External AAA Authentication Services with DHCP | 833 |
| Creating Unique Usernames for DHCP Clients | 834 |
**client-identifier (DHCP Client)**

**Syntax**

```plaintext
client-identifier {
    user-id { ascii ascii hexadecimal hexadecimal;
    use-interface-description {logical | device};
    prefix [host-name routing-instance-name];
}
```

**Hierarchy Level**

```plaintext
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

**Description**

The DHCP server identifies a client by a client-identifier value.

**Options**

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- DHCPv6 Client Overview | 998
client-identifier (DHCPv6 Client)

Syntax

client-identifier duid-type (duid-ll | duid-llt | vendor);

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]

Release Information
Statement introduced in Junos OS Release 12.1X45-D10. The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description
The DHCPv6 server identifies a client by a client-identifier value.

Options
duid-type—The DHCPv6 client is identified by a DHCP unique identifier (DUID).

duid-ll—Link Layer address.

duid-llt—Link Layer address plus time.

vendor—Vendor-assigned unique ID based on the enterprise number.

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

RELATED DOCUMENTATION

| DHCPv6 Client Overview | 998 |
client-list-name

Syntax

```
client-list-name client-list-name;
```

Hierarchy Level

```
[edit snmp community community-name]
```

Release Information
Statement introduced in Junos OS Release 8.5 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Add a client list or prefix list to an SNMP community.

Options
`client-list-name`—Name of the client list or prefix list.

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

RELATED DOCUMENTATION

`Adding a Group of Clients to an SNMP Community`
client-list-name (SNMP)

Syntax

```
client-list-name  client-list-name ;
```

Hierarchy Level

```
[edit snmp community  community-name ]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the name of the list of SNMP network management system (NSM) clients that are authorized to collect information about network operations. You cannot use an SNMP client list and individually configured SNMP clients in the same configuration.

Options

```
client-list-name — Name of the client list. Client list is the list of IP address prefixes defined with the prefix-list statement in the policy-options hierarchy.
```

Required Privilege Level

```
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.
```
**client-type**

Syntax

```plaintext
client-type (autoconfig | stateful);
```

Hierarchy Level

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

Description

The type of DHCPv6 client.

Options

- `autoconfig`—Autoconfig client type for router advertisement
- `stateful`—Stateful client type for address assignment

Required Privilege Level

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

**RELATED DOCUMENTATION**

- DHCPv6 Client Overview | 998
clients

Syntax

clients {
  address <restrict>;
}

Hierarchy Level
[[edit snmp community community community-name]]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

Default
If you omit the clients statement, all SNMP clients using this community string are authorized to access the router.

Options
address—Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple address options.

restrict—(Optional) Do not allow the specified SNMP client to access the router.

Required Privilege Level
snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Configuring SNMP Communities
coa-immediate-update

Syntax

coa-immediate-update;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Configure the router to send an Acct-Update message to the RADIUS accounting server immediately following a CoA operation.

Required Privilege Level

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

RELATED DOCUMENTATION

RADIUS Servers and Parameters for Subscriber Access
Configuring Per-Subscriber Session Accounting
coa-no-override service-class-attribute

Syntax

coa-no-override service-class-attribute;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Specify that, after a CoA action that changes the RADIUS Class attribute, accounting reports for the subscriber’s service sessions continue to use the original Class attribute that was assigned when the service sessions were created. The new Class attribute value is used in accounting reports for the subscriber session only.

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

RELATED DOCUMENTATION

* RADIUS Servers and Parameters for Subscriber Access
* Configuring Per-Subscriber Session Accounting
commit-delay

Syntax

commit-delay seconds;

Hierarchy Level

[edit snmp nonvolatile]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series switches.

Description
Configure the timer for the SNMP Set reply and start of the commit.

Options
seconds—Delay between an affirmative SNMP Set reply and start of the commit.

Default: 5 seconds

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

RELATED DOCUMENTATION

Configuring the Commit Delay Timer
community (SNMP)

Syntax

```
community community-name [ 
    authorization authorization;
    client-list-name client-list-name;
    clients {
        address restrict;
    }
    view view-name;
]
```

Hierarchy Level

```
[edit snmp]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

NOTE: The `authorization read-write` option is not supported on the QFX3000 QFabric system.

The SNMP client application specifies an SNMP community name in `Get`, `GetBulk`, `GetNext`, and `Set` SNMP requests.

Default
If you omit the `community` statement, all SNMP requests are denied.

Options
`community-name`—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring SNMP Communities
- Configuring the SNMP Community String

---

**compress (Accounting Options)**

**Syntax**

```
compress;
```

**Hierarchy Level**

```
[edit accounting-options file filename]
```

**Release Information**


**Description**

Compress the accounting file during file transfer to the backup site.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring Accounting-Data Log Files
- Configuring Flat-File Accounting for Layer 2 Wholesale
- Configuring Flat-File Accounting for Extensible Subscriber Services Management
- Flat-File Accounting Overview
### connection-limit

#### Syntax

```plaintext
connection-limit limit;
```

#### Hierarchy Level

```
[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]
```

#### Release Information

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

#### Description

Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

#### Options

- **limit**—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

```
Range: 1 through 250
Default: 75
```

---

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured `connection-limit` value if the system resources are limited.

#### Required Privilege Level

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

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications

Configuring DTCP-over-SSH Service for the Flow-Tap Application

Configuring Finger Service for Remote Access to the Router | 294

Configuring FTP Service for Remote Access to the Router or Switch | 293

Configuring SSH Service for Remote Access to the Router or Switch | 294

Configuring Telnet Service for Remote Access to a Router or Switch | 292
connection-limit

Syntax

connection-limit limit;

Hierarchy Level

[edit system services finger]
[edit system services ftp]
[edit system services netconf ssh]
[edit system services ssh]
[edit system services telnet]
[edit system services xnm-clear-text]
[edit system services xnm-ssl]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Configure the maximum number of connection sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options
limit—Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250
Default: 75

NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.

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

Syntax

contact contact;

Hierarchy Level

[edit snmp]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series Routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Defines the value of the SNMP MIB II sysContact object, which is the contact person for the managed system.

Options

contact—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

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

RELATED DOCUMENTATION

Configuring the System Contact on a Device Running Junos OS
counters

Syntax

counters {
     counter-name;
}

Hierarchy Level

[edit accounting-options filter-profile profile-name]

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

Description
Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the /var/log directory.

Options

counter-name—Name of the counter.

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

RELATED DOCUMENTATION

Configuring the Counters
country-code

Syntax

```
country-code code;
```

Hierarchy Level

```
[edit protocols lldp-med interface (all | interface-name)]
```

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the two-letter country code to include in the location information. Location information is advertised from the switch to the MED, and is used during emergency calls to identify the location of the MED. The country code is required when configuring LLDP-MED based on location.

Default

Disabled.

Options

code—Two-letter ISO 3166 country code in capital ASCII letters; for example, US or DE.

Required Privilege Level

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

RELATED DOCUMENTATION

- show lldp | 2680
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Configuring LLDP-MED (CLI Procedure) | 665
crl (Encryption Interface)

Syntax

crl file-name;

Hierarchy Level

[edit security certificates]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options

file-name—Specify the file from which to read the CRL.

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

RELATED DOCUMENTATION

Configuring the Certificate Authority Properties for an ES PIC
custom-options

Syntax

```plaintext
custom-options {
    banner-message string;
    footer-bgcolor color;
    footer-message string;
    footer-text-color color;
    form-header-bgcolor color;
    form-header-message string;
    form-header-text-color color;
    form-reset-label label name;
    form-submit-label label name;
    header-bgcolor color;
    header-logo filename;
    header-message string;
    header-text-color color;
    post-authentication-url url-string;
}
```

Hierarchy Level

[edit services captive-portal]

Release Information
Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description
Specify the design elements of a captive portal login page.

Options

**banner-message**—The first screen displayed before the captive portal login page is displayed—for example, a disclaimer message.

Range: 1–2047 characters

**footer-bgcolor**—The hexadecimal color code for the color of the footer bar across the bottom of the captive portal login page—for example, #2E8B57 (sea green).

Values: # symbol followed by six characters.

**footer-message**—Text message displayed in the footer bar across the bottom of the captive portal login page.

Range: 1–2047 characters
Default: Copyright @2010, Juniper Networks Inc.

**footer-text-color** — Color of the text in the footer.

Default: The default color is white.

**form-header-bgc** — The hexadecimal color code for the background color of the header bar across the top of the form area of the captive portal login page.

Values: # symbol followed by six characters.

**form-header-message** — Text message displayed in the header bar across the top of the form area of the captive portal login page.

Range: 1–255 characters

Default: Captive Portal User Authentication

**form-header-text-color** — Color of the text in the form header.

Default: The default color is black.

**form-reset-label** — Label displayed in the button that the user can select to clear the username and password fields on the form.

Range: 1–255 characters

Default: Reset

**form-submit-label** — Label displayed in the button that the user selects to submit their login information—for example, Log In.

Range: 1–255 characters

Default: Log In

**header-bgc** — The hexadecimal color code for the color of the header bar across the top of the captive portal login page.

Values: # symbol followed by six characters.

**header-logo** — Filename of the file containing the image of the logo displayed at the top of the captive portal login page. The image file can be in GIF, JPEG, or PNG format.

Default: The Juniper Networks logo

**header-message** — Text displayed in the header bar across the bottom of the captive portal login page.

Range: 1–2047 characters

Default: User Authentication

**header-text-color** — Color of the text in the header.

Default: The default color is white.
**post-authentication-url**—URL to which the users are directed upon successful authentication—for example www.mycafe.com.

**Range:** 1–255 characters

**Default:** The page originally requested by the user.

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

**RELATED DOCUMENTATION**

- Designing a Captive Portal Authentication Login Page on Switches | 494
- Configuring Captive Portal Authentication (CLI Procedure) | 492
## delegated-pool (DHCP Local Server)

### Syntax

```
delegated-pool pool-name;
```

### Hierarchy Level

- [edit system services dhcp-local-server dhcpv6 overrides],
- [edit system services dhcp-local-server dhcpv6 group group-name overrides],
- [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...],
- [edit logical-systems logical-system-name system services system services dhcp-local-server dhcpv6 ...],
- [edit routing-instances routing-instance-name system services system services dhcp-local-server dhcpv6 ...]

### Release Information

- Statement introduced in Junos OS Release 11.4.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

### Description

Specify the address pool that assigns the IA_PD address. A pool specified by RADIUS VSA 26-161 takes precedence over the pool specified by this `delegated-pool` statement.

### Options

- `pool-name`—Name of the address-assignment pool.

### Required Privilege Level

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

### RELATED DOCUMENTATION

- *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*
- *Overriding the Default DHCP Local Server Configuration Settings Overview*
delimiter (DHCP Local Server)

Syntax

```
delimiter delimiter-character;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the character used as the delimiter between the concatenated components of the username.

Options
delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Default: . (period)

NOTE: When you include the interface-description in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is configured as "Backbone connection/PHL01", you cannot use the forward slash (/) as the delimiter.

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

RELATED DOCUMENTATION
Using External AAA Authentication Services with DHCP | 833
delimiter (DHCP Relay Agent)

Syntax

delimiter delimiter-character;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description
Specify the character used as the delimiter between the concatenated components of the username. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

**delimiter-character**—Character that separates components that make up the concatenated username. You cannot use the semicolon (:) as a delimiter.

**Default:** . (period)

**NOTE:** When you include the **interface-description** in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is configured as "Backbone connection/PHL01", you cannot use the forward slash (/) as the delimiter.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- [Using External AAA Authentication Services with DHCP](#) | 833
- [Creating Unique Usernames for DHCP Clients](#) | 834
description (Authentication Keychain)

Syntax

description text-string;

Hierarchy Level

[edit security authentication-key-chains key-chain key-chain-name]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description

Configure a description for an authentication key-chain.

Options

text-string—A text string describing the authentication-key-chain. Put the text string in quotes ("text description").

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols | 286
Example: Configuring BFD Authentication for Securing Static Routes
Example: Configuring Hitless Authentication Key Rollover for IS-IS
destination (Accounting)

Syntax

destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        max-outstanding-requests value;
        port port-number;
        retry value;
        secret password;
        source-address source-address;
        timeout seconds;
      }
    }
  }
}

tacplus {
  server {
    server-address {
      port port-number;
      secret password;
      single-connection;
      timeout seconds;
    }
  }
}

Hierarchy Level

[edit system accounting]

Release Information
Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4. Support for IPv6 source address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description
Configure the authentication server.

Options
The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
destination (Accounting)

Syntax

destination {
  radius {
    server {
      server-address {
        accounting-port port-number;
        retry number;
        routing-instance routing-instance;
        secret password;
        source-address address;
        source-address-inet6 IPv6-source-address;
        timeout seconds;
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        routing-instance routing-instance;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
}

Hierarchy Level

[edit system accounting]

Release Information
Statement introduced before Junos OS Release 7.4.
radius statement added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure the authentication server.

Options

source-address-inet6 IPv6-source-address—A valid IPv6 address configured on one of the routers or switch interfaces.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS System Accounting | 255
- Configuring TACACS+ System Accounting | 278
destination (RADSEC)

Syntax

    destination id-number {    
        address ip-address;    
        max-tx-buffers number;    
    }

Hierarchy Level

    [edit access radsec]

Release Information

Statement introduced in Junos OS Release 19.1R1.

Description

Define the RADSEC server as a destination for RADIUS traffic. Traffic that is destined for a RADIUS server can then be redirected to the RADSEC destination. RADSEC destinations are identified by a unique numeric ID. You can configure multiple RADSEC destinations with different parameters pointing to the same RADSEC server.

Options

- **id-number**—Globally unique ID number for the RADSEC destination.
- **address ip-address**—IP address of the RADSEC server.
- **max-tx-buffers number**—Maximum number of packets buffered on transmission.

    NOTE: The buffer allocation should be able to accommodate the **max-outstanding-requests** for mapped RADIUS servers configured at the [edit access radius-server] hierarchy level.

Range: 32 through 32000
Default: 100

Required Privilege Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.
destination-classes

Syntax

```
destination-classes {
    destination-class-name;
}
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the destination classes for which statistics are collected.

Options

`destination-class-name`—Name of the destination class to include in the source class usage profile.

Required Privilege Level

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

RELATED DOCUMENTATION

`Configuring a Class Usage Profile`
destination-host (Gx-Plus)

Syntax

```
destination-host hostname;
```

Hierarchy Level

```
[edit access gx-plus partition partition-name]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the host on which the PCRF application resides.

Options

`hostname`—Host on which the PCRF is installed.

Required Privilege Level

admin—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Configuring Gx-Plus
- Configuring the Gx-Plus Partition
destination-realm (Gx-Plus)

Syntax

destination-realm realm;

Hierarchy Level

[edit access gx-plus partition partition-name]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the realm in which the PCRF host resides.

Options

realm—Realm in which the PCRF host resides.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Gx-Plus

Configuring the Gx-Plus Partition
**detection-time**

**Syntax**

```plaintext
detection-time {
    threshold milliseconds;
}
```

**Hierarchy Level**

- [edit system services dhcp-local-server liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
- [edit forwarding-options dhcp-relay liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
- [edit system services dhcp-local-server group group-name liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Enable failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
dhcp

Syntax

dhcp {
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time seconds;
    domain-name domain-name;
    domain-search [domain-list];
    maximum-lease-time seconds;
    name-server {
        address;
    }
    next-server next-server
    option option-identifier-code ;
    pool address/prefix-length {
        address-range {
            low address;
            high address;
        }
        exclude-address {
            address;
        }
    }
    router {
        address;
    }
    static-binding mac-address {
        fixed-address {
            address;
        }
        host-name hostname;
        client-identifier (ascii client-id | hexadecimal client-id);
    }
    wins-server {
        address;
    }
}

Hierarchy Level

[edit system services]
[edit logical-systems logical-system-name system services]

Release Information
Statement introduced before Junos OS Release 7.4.
The logical-systems option is introduced in Junos OS Release 18.4R1.

Description
Configure a router, or a switch as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

System Management Configuration Statements
Example: Complete DHCP Server Configuration | 708
dhcp (DHCP Client)

Syntax

```snippet
dhcp {
    client-identifier duid-type (duid-ll | duid-llt | vendor);
    no-dns-install;
    rapid-commit;
    options name;
}
```

Hierarchy Level

```snippet
[edit interfaces interface-name unit logical-unit-number family inet]
[edit logical-systems name interfaces interface-name unit logical-unit-number family inet]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches. The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description

Configure a Dynamic Host Configuration Protocol (DHCP) client for an IPv4 interface for logical systems and tenant systems.

The remaining statements are described separately.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, mgmt_junos.

Options

client-identifier duid-type—Identify a client by a client-identifier value. This statement is mandatory.

no-dns-install—Configure the DHCPv6 client DNS information.

options—Specify options requested by the DHCPv4 client.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

Configuring a DHCP Client (CLI Procedure) | 762
dhcp-attributes (Access IPv4 Address Pools)

Syntax

dhcp-attributes {
  boot-file boot-file-name;
  boot-server boot-server-name;
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  name-server ipv4-address;
  netbios-node-type (b-node | h-node | m-node | p-node);
  next-server next-server-name;
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [false | on | true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag (false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  option-match {
    option-82 {
      circuit-id match-value {
        range range-name;
      }
      remote-id match-value {
        range range-name;
      }
    }
  }
  propagate-ppp-settings [interface-name];
}
propagate-settings interface-name;
router ipv4-address;
server-identifier ip-address;
sip-server {
ip-address ipv4-address;
name sip-server-name;
}
tftp-server server-name;
wins-server ipv4-address;
}

Hierarchy Level
[edit access address-assignment pool pool-name family inet]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.

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

RELATED DOCUMENTATION
| DHCP Overview | 909 |
**dhcp-attributes (Access IPv6 Address Pools)**

**Syntax**

```plaintext
dhcp-attributes {
  dns-server ipv6-address;
  grace-period seconds;
  maximum-lease-time (seconds | infinite);
  option dhcp-option-identifier-code {
    array {
      byte [8-bit-value];
      flag [false | off | on | true];
      integer [32-bit-numeric-values];
      ip-address [ip-address];
      short [signed-16-bit-numeric-value];
      string [character string value];
      unsigned-integer [unsigned-32-bit-numeric-value];
      unsigned-short [16-bit-numeric-value];
    }
    byte 8-bit-value;
    flag (false | off | on | true);
    integer 32-bit-numeric-values;
    ip-address ip-address;
    short signed-16-bit-numeric-value;
    string character string value;
    unsigned-integer unsigned-32-bit-numeric-value;
    unsigned-short 16-bit-numeric-value;
  }
  propagate-ppp-settings [interface-name];
  sip-server-address ipv6-address;
  sip-server-domain-name domain-name;
}
```

**Hierarchy Level**

```
[edit access address-assignment pool pool-name family inet6]
```

**Release Information**

Statement introduced in Junos OS Release 10.4.

**Description**

Configure attributes for address pools that can be used by different clients.

**Options**
• **dns-server IPv6-address**—Specify a DNS server to which clients can send DNS queries.

• **grace-period seconds**—Specify the grace period offered with the lease.

Range: 0 through 4,294,967,295 seconds

Default: 0 (no grace period)

• **maximum-lease-time seconds**—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

Range: 30 through 4,294,967,295 seconds

Default: 86,400 seconds (24 hours)

• **option dhcp-option-identifier-code**—Specify the DHCP option identifier code.

• **propagate-ppp-settings [interface-name]**—Specify PPP interface name for propagating DNS or WINS settings.

• **sip-server-address IPv6-address**—Specify the IPv6 address of the SIP outbound proxy server.

• **sip-server-domain-name domain-name**—Specify the domain name of the SIP outbound proxy server.

**Required Privilege Level**

access—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

| DHCP Overview | 909 |
dhcp-client

Syntax

dhcp-client {
  client-identifier {
    prefix {
      host-name;
      logical-system-name;
      routing-instance-name;
    }
    use-interface-description (device | logical);
    user-id (ascii string| hexadecimal string);
  }
  force-discover;
  lease-time (length | infinite);
  no-dns-install;
  options no-hostname;
  retransmission-attempt value;
  retransmission-interval seconds;
  server-address server-address;
  update-server;
  vendor-id vendor-id ;
}

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.4R1 and Junos OS Release 15.1X49-D60, on all SRX Series devices and vSRX instances, the CLI option dhcp-client at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to align with other Junos platforms. There is no change in the functionality.

Description
Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options
- **force-discover**—Forces the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client.

- **lease-time**—Specify the time to negotiate and exchange DHCP information.
  - **infinite**—Lease never expires.
  - **length**—Number of seconds.

- **no-dns-install**—Do not add DNS information to the DHCP client (resolve.conf) even after learn from DHCP server

- **retransmission-attempt**—Specify the number of times the device attempts to retransmit a DHCP packet fallback. Range is 0-6.

- **server-address**—Specify the preferred DHCP server address that is sent to DHCP clients.

- **update-server**—Propagate TCP/IP settings to a local DHCP server.

- **vendor-id**—Vendor class ID for the DHCP client.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- DHCP Overview | 909
dhcp-local-server

Syntax

dhcp-local-server {
    access-profile profile-name;
    allow-active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
    }
    allow-bulk-leasequery {
        max-connections number-of-connections;
        max-empty-replies number-of-replies;
        restricted-requestor;
        timeout seconds;
    }
    allow-leasequery {
        restricted-requestor;
    }
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    dhcpv6 {
        access-profile profile-name;
        allow-active-leasequery {
            idle-timeout seconds;
            peer-address address;
            timeout seconds;
        }
    }
}
allow-bulk-leasequery {
    max-connections number-of-connections;
    max-empty-replies number-of-replies;
    restricted-requestor;
    timeout seconds;
}
allow-leasequery {
    restricted-requestor;
}
authentication {
    ...
}
duplicate-clients incoming-interface;
group group-name {
    access-profile profile-name;
    authentication {
        ...
    }
}
interface interface-name {
    access-profile profile-name;
    exclude;
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
        }
        delay-time seconds;
    }
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
method {
    bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        detection-time {
            threshold milliseconds;
        }
        session-mode (automatic | multihoop | singlehop);
        holddown-interval milliseconds;
    }
    layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
    }
}
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
        }
        delay-time seconds;
    }
    delegated-pool;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
} 
route-suppression;
server-duid-type type;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            delay-time seconds;
        }
    }
    delegated-pool;
    dual-stack dual-stack-group-name;
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
support-option-pd-exclude;
timeout timeout-value;
token token-value;
  trigger {
    radius-disconnect;
  }
}

reauthenticate (lease-renewal remote-id-mismatch);
requested-ip-network-match subnet-mask;
route-suppression;
server-lduid-type type;
service-profile dynamic-profile-name;
short-cycle-protection lockout-min-time lockout-max-time;
}
dual-stack-group name {
  access-profile access-profile;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
  }
  dual-stack-interface-client-limit number;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  on-demand-address-allocation;
  protocol-master (inet | inet6);
  reauthenticate (<lease-renewal> <remote-id-mismatch>);
  service-profile service-profile;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
duplicate-clients-in-subnet (incoming-interface | option-82);

dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name>;

forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
    authentication {
        ...
    }
}
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name>;
interface interface-name {
    exclude;
    overrides {
        asymmetric-lease-time seconds;
        client-discover-match (option60-and-option82 | incoming-interface);
        delay-offer {
            based-on (option-60 | option-77 | option-82) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        include-option-82 {
            forcerenew;
            nak;
        }
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
}
liveness-detection {
failure-action (clear-binding | clear-binding-if-interface-up | log-only);
method {
  bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    detection-time {
      threshold milliseconds;
    }
    session-mode (automatic | multihop | singlehop);
    hold-down-interval milliseconds;
  }
  layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval interval;
  }
}
}
overrides {
  asymmetric-lease-time seconds;
  client-discover-match (option60-and-option82 | incoming-interface);
  delay-offer {
    based-on (option-60 | option-77 | option-82) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  } 
  include-option-82 {
    forcerenew;
    nak;
  }
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  protocol-attributes attribute-set-name;
}
requested-ip-network-match subnet-mask
route-suppression;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}

on-demand-address-allocation;
overrides {
  asymmetric-lease-time seconds;
  client-discover-match <option60-and-option82 | incoming-interface>;
  delay-offer {
    based-on (option-60 | option-77 | option-82) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  protocol-attributes attribute-set-name;
}
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
}
protocol-master;
reauthenticate (<lease-renewal> <remote-id-mismatch>);
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
requested-ip-network-match subnet-mask;
route-suppression;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services],
[edit logical-systems logical-system-name system services],
[edit routing-instances routing-instance-name system services],
[edit system services]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch to enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and, therefore, is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the [edit forwarding-options helpers] hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The dhcpv6 stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.

NOTE: When you configure the dhcp-local-server statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Extended DHCP Local Server Overview | 718
- DHCPv6 Local Server Overview | 787
dhcp-local-server (System Services)

Syntax

dhcp-local-server {
  dhcpv6 {
    authentication {
      password password;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix;
      }
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
  }
  junos-default-profile;
  use-primary dynamic-profile-name;
}

group group-name {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
    }
  }
}
routing-instance-name;
user-prefix user-prefix;
}
}
dynamic-profile {
    profile-name;
    aggregate-clients {
        merge;
        replace;
    }
    junos-default-profile;
    use-primary dynamic-profile;
}
interface interface-name {
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    exclude;
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    service-profile service-profile-name
    trace ;
    upto interface-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
    }
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
  service-profile service-profile-name;
}
group group-name {  
    interface interface-name {  
        exclude;  
        upto upto-interface-name;  
    }  
}  
}

Hierarchy Level
[edit system services]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.

NOTE: SRX Series devices do not support client authentication.

Options
The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION
- DHCP Overview | 909
dhcp-relay

Syntax

dhcp-relay {
    access-profile profile-name;
    active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
        topology-discovery;
    }
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    bulk-leasequery {
        attempts number-of-attempts;
        timeout seconds;
    }
    dhcpv6 {
        access-profile profile-name;
        active-leasequery {
            idle-timeout seconds;
            peer-address address;
            timeout seconds;
            topology-discovery;
        }
        active-server-group server-group-name;
    }
}
authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description (device-interface | logical-interface);
    interface-name interface-name;
    logical-system-name;
    mac-address mac-address;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
  }
}
bulk-leasequery {
  attempts number-of-attempts;
  timeout seconds;
  trigger automatic;
}
duplicate-clients incoming-interface;
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
forward-only {
  logical-system <current | default | logical-system-name>;
  routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name interface-name;
            logical-system-name;
            mac-address mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
}
forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
interface interface-name {
    access-profile profile-name;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    exclude;
    overrides {
        allow-snooped-clients;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-authentication;
        delete-binding-on-renegotiation;
dual-stack dual-stack-group-name;
interface-client-limit number;
no-allow-snooped-clients;
no-bind-on-request;
relay-source interface-name;
send-release-on-delete;
}

service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
}
}
lease-time-validation {
  lease-time-threshold seconds;
  violation-action action;
}

liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
  }
}
}
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-interface-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
remote-id-mismatch disconnect;
route-suppression;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
leasequery {
  attempts number-of-attempts;
  timeout seconds;
}
lease-time-validation {
  lease-time-threshold seconds;
  violation-action action;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
        route-suppression;
        service-profile dynamic-profile-name;
    }
}

no-snoop;
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
relay-option-vendor-specific{
    host-name;
    location;
    remote-id-mismatch disconnect;
    route-suppression;
server-group {
  server-group-name {
  server-ip-address;
  }
}
server-response-time seconds;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
dual-stack-group dual-stack-group-name {
  access-profile profile-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
  }
  dual-stack-interface-client-limit number;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  protocol-master (inet | inet6);
  relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
use-interface-description (logical | device);
use-option-82 <strict>;
use-vlan-id;
}
relay-agent-remote-id {
 include-irb-and-l2;
 keep-incoming-remote-id;
 no-vlan-interface-name;
 prefix prefix;
 use-interface-description (logical | device);
 use-option-82 <strict>;
 use-vlan-id;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
duplicate-clients-in-subnet (incoming-interface | option-82):
dynamic-profile profile-name [
 aggregate-clients (merge | replace);
 use-primary primary-profile-name;
]
forward-only {
 logical-system <current | default | logical-system-name>;
 routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
  access-profile profile-name;
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description (device-interface | logical-interface);
      interface-name interface-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 [circuit-id] [remote-id];
      routing-instance-name;
      user-prefix user-prefix-string;
    }
    vlan-tags;
  }
}

dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}

forward-only {
  logical-system <current | default | logical-system-name>;
  routing-instance <current | default | routing-instance-name>;
}

forward-only {
  logical-system <current | default | logical-system-name>;
  routing-instance <current | default | routing-instance-name>;
}

interface interface-name {
  access-profile profile-name;
  exclude;
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
      }
    }
  }
}
transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
}
detection-time {
    threshold milliseconds;
}
session-mode (automatic | multihop | singlehop);
holddown-interval milliseconds;
}

overrides {
    allow-no-end-option;
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
}
overrides {
    allow-no-end-option
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group group-name;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {  
circuit-id {  
  prefix prefix;  
  use-interface-description (logical | device);  
}  
remote-id {  
  prefix prefix;  
  use-interface-description (logical | device);  
}  
server-id-override
}
remote-id-mismatch disconnect;
route-suppression:
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
leasequery {  
  attempts number-of-attempts;
  timeout seconds;
}
lease-time-validation {  
  lease-time-threshold seconds;
  violation-action action;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
  }
}
}
no-snoop;
overrides {
    allow-no-end-option
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group group-name;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
  remote-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
  server-id-override
}
remote-id-mismatch disconnect;
route-suppression:
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
  server-response-time seconds;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}

Hierarchy Level

[edit forwarding-options],
[edit logical-systems logical-system-name forwarding-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options],
[edit routing-instances routing-instance-name forwarding-options]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description
Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch to enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

The extended DHCP and DHCPv6 relay agent options configured with the `dhcp-relay` and `dhcpv6` statements are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

| Extended DHCP Relay Agent Overview | 792 |
| DHCPv6 Relay Agent Overview       | 829 |
| DHCP Relay Proxy Overview         | 826 |
| Using External AAA Authentication Services with DHCP | 833 |
dhcp-service

Syntax

dhcp-service {
    accept-max-tcp-connections max-tcp-connections;
    dhcp-snooping-file(local_pathname | remote_URL) {
        write-interval interval;
    }
    dhcpv6-snooping-file {
        location;
        write-interval seconds;
    }
    (disable | enable);
    interface-traceoptions {
        file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        level (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
    log {
        session {
            client;
            all;
            dhcpv6 {
                client;
                server;
                relay;
                dynamic-server;
                all;
            }
            server;
            relay;
        }
        server;
        relay;
    }
    ltv-syslog-interval seconds;
    persistent-storage {
        backup-interval backup-interval;
        file-name;
    }
    request-max-tcp-connections max-tcp-connections;
    traceoptions {
        traceoptions
    }
Hierarchy Level

[edit system processes]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1 for MX Series routers.
Support for log option introduced in Junos OS Release 19.1R1 for SRX Series devices.

Description
Enable DHCP services on the device. DHCP services automate network-parameter assignment to network
devices. The DHCP service process is enabled by default. However, by default, IP-MAC bindings in the
DHCP snooping database do not persist through device reboots. You can improve performance after
rebooting by configuring the IP-MAC bindings to persist, by configuring a storage location for the DHCP
database file. When specifying the location for the DHCP database, you must also specify how frequently
the switch writes the database entries into the DHCP snooping database file.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked
statement in the Syntax section for details.

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

RELATED DOCUMENTATION

Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)
dhcpv6 (DHCP Local Server)

Syntax

dhcpv6 {
    access-profile profile-name;
    allow-active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
    }
    allow-bulk-leasequery {
        max-connections number-of-connections;
        max-empty-replies number-of-replies;
        restricted-requestor;
        timeout seconds;
    }
    allow-leasequery {
        restricted-requestor;
    }
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    duplicate-clients incoming-interface;
    group group-name {
        access-profile profile-name;
        authentication {
            ...
        }
        interface interface-name [

access-profile profile-name;
exclude;
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            delay-time seconds;
        }
        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
        }
        delay-time seconds;
    }
    delegated-pool;
    delete-binding-on-renegotiation;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      };
      detection-time {
        threshold milliseconds;
      };
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
  }
}
}
overrides {
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-negotiation-match incoming-interface;
  delay-advertise {
    based-on (option-15 | option-16 | option-18 | option-37) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  delegated-pool;
  delete-binding-on-renegotiation;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  protocol-attributes attribute-set-name;
  rapid-commit;
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
}
reauthenticate (<lease-renewal> <remote-id-mismatch>);
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    support-option-pd-exclude;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
requested-ip-network-match subnet-mask;
route-suppression;
server-duid-type type;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Configure DHCPv6 local server options on the router or switch to enable the router or switch to function as a server for the DHCP protocol for IPv6. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

DHCPv6 Local Server Overview | 787
dhcpv6 (DHCP Relay Agent)

Syntax

dhcpv6 {
    access-profile profile-name;
    active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
        topology-discovery;
    }
    active-server-group server-group-name;
}

authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description (device-interface | logical-interface);
        interface-name interface-name;
        logical-system-name;
        mac-address mac-address;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
    }
}

bulk-leasequery {
    attempts number-of-attempts;
    timeout seconds;
    trigger automatic;
}

duplicate-clients incoming-interface;

dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}

forward-only {

logical-system <current | default | logical-system-name>;
  routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
}
forward-snoopened-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
  access-profile profile-name;
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-description (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
}
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
forward-only {
  logical-system <current | default | logical-system-name>;
  routing-instance <current | default | routing-instance-name>;
}
interface interface-name {
  access-profile profile-name;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  exclude;
  overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
dual-stack dual-stack-group-name;
interface-client-limit number;
no-allow-snooped-clients;
no-bind-on-request;
relay-source interface-name;
send-release-on-delete;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
}
}
lease-time-validation {
 lease-time-threshold seconds;
 violation-action action;
}
liveness-detection {
 failure-action (clear-binding | clear-binding-if-interface-up | log-only);
 method {
   bfd {
       version (0 | 1 | automatic);
       minimum-interval milliseconds;
       minimum-receive-interval milliseconds;
       multiplier number;
       no-adaptation;
       transmit-interval {
           minimum-interval milliseconds;
           threshold milliseconds;
       }
       detection-time {
           threshold milliseconds;
       }
       session-mode (automatic | multihop | singlehop);
       holddown-interval milliseconds;
   }
   layer2-liveness-detection {
       max-consecutive-retries number;
       transmit-interval interval;
   }
}
}
}
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict> ;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  remote-id-mismatch disconnect;
  route-suppression;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
leasequery {
  attempts number-of-attempts;
  timeout seconds;
}
lease-time-validation {
  lease-time-threshold seconds;
  violation-action action;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
    route-suppression;
    service-profile dynamic-profile-name;
  }
}
no-snoop;
overrides {
  allow-snooped-clients;
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-negotiation-match incoming-interface;
  delay-authentication;
  delete-binding-on-renegotiation;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  no-allow-snooped-clients;
  no-bind-on-request;
  relay-source interface-name;
  send-release-on-delete;
}
relay-agent-interface-id {
  include-irb-and-l2;
  keep-incoming-interface-id;
  no-vlan-interface-name;
  prefix prefix;
  use-interface-description (logical | device);
  use-option-82;
}
relay-agent-remote-id {
  include-irb-and-l2;
  keep-incoming-interface-id;
  no-vlan-interface-name;
  prefix prefix;
  use-interface-description (logical | device);
  use-option-82 <strict>;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
}
relay-option-vendor-specific {
  host-name;
  location;
  remote-id-mismatch disconnect;
  route-suppression;
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
}
server-response-time seconds;
  service-profile dynamic-profile-name;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support for forward-snooped-clients introduced in Junos OS Release 15.1X53-D56 for EX Series switches and Junos OS Release 17.1R1.

Description
Configure DHCPv6 relay options on the router or switch and enable the router or switch to function as a DHCPv6 relay agent. A DHCPv6 relay agent forwards DHCPv6 request and reply packets between a DHCPv6 client and a DHCPv6 server.

The DHCPv6 relay agent server is fully compatible with the extended DHCP local server and DHCP relay agent. However, the options configured with the dhcpv6 statement are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, the DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot be enabled on the router or switch at the same time.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

dhcp-relay | 1665
DHCPv6 Relay Agent Overview | 829
Using External AAA Authentication Services with DHCP | 833
dhcpv6 (System Services)

Syntax

dhcpv6 {
  authentication {
    password password;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix;
    }
  }
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  group group-name {
    authentication {
      password password;
      username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
      }
    }
  }
}
user-prefix user-prefix;
}
}
dynamic-profile {
  profile-name;
  aggregate-clients {
    merge;
    replace;
  }
  junos-default-profile;
  use-primary dynamic-profile;
}
interface interface-name {
  dynamic-profile {
    profile-name;
    aggregate-clients {
      merge;
      replace;
    }
    junos-default-profile;
    use-primary dynamic-profile-name;
  }
  exclude;
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  service-profile service-profile-name
  trace ;
  upto interface-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
  service-profile service-profile-name;
}
liveness-detection {
  failure-action {
    clear-binding;
    clear-binding-if-interface-up;
    log-only;
  }
  method {
    bfd {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval interval;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      session-mode (automatic | multihop | single-hop);
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
  }
  overrides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit ;
  }
  reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
      radius-disconnect;
    }
  }
  service-profile service-profile-name;
}
Hierarchy Level

[edit system services]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure DHCPv6 server to provide IPv6 addresses to clients.

NOTE: SRX Series devices do not support client authentication.

Options
- duplicate-clients-on-interface—Allow duplicate clients on different interfaces in a subnet.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

DHCP Overview | 909
dhcppv6-client

Syntax

dhcppv6-client {
  client-ia-type {
    ia-na;
    ia-pd;
  }
  client-identifier duid-type (duid-ll | duid-lit | vendor);
  client-type (autoconfig | stateful);
  rapid-commit;
  req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);
  retransmission-attempt number;
  update-router-advertisement {
    interface interface-name;
  }
  update-server;
}

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet6]
[edit logical-systems name interfaces name unit name family inet6]
[edit tenants tenant-name interfaces name unit name family inet6]

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description

Configure the Dynamic Host Configuration Protocol version 6 (DHCPPv6) client.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, mgmt_junos.

Options

client-ia-type— Identity association type for DHCPv6 client. This statement is mandatory.
**client-identifier duid-type**— Identity a client by a client-identifier value. This statement is mandatory.

**client-type**— Identify the type of DHCPv6 client. This statement is mandatory.

**rapid-commit**— The use of the two-message exchange for address assignment.

**req-option**— Specify options requested by the DHCPv6 client.

**retransmission-attempt number**— Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

**update-router-advertisement**— Specify the interface used to delegate prefixes.

**update-server**— Propagate TCP/IP settings to the DHCPv6 server.

For detailed information about these commands, see CLI Explorer.

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

**RELATED DOCUMENTATION**

| DHCP Overview | 909 |
| Minimum DHCPv6 Client Configuration | 998 |
diameter-instance (Diameter Applications)

Syntax

diameter-instance instance-name;

Hierarchy Level

[edit access gx-plus partition partition-name]
[edit access ocs partition partition-name],
[edit access pcrf partition partition-name]

Release Information
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support at the [edit access ocs partition partition-name] and [edit access pcrf partition partition-name] hierarchy levels introduced in Junos OS Release 16.2.

Description
Specify the Diameter instance associated with the Gx-Plus, OCS, or PCRF partition.

Options
instance-name—Name of the Diameter instance. Currently, only master is supported.

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

RELATED DOCUMENTATION

Configuring Gx-Plus
Configuring the Gx-Plus Partition
Configuring the OCS Partition
Understanding Gx Interactions Between the Router and the PCRF
Understanding Gy Interactions Between the Router and the OCS
disable (802.1X)

Syntax

disable;

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names])]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Disable 802.1X authentication on a specified interface or all interfaces.

Default
802.1X authentication is disabled on all interfaces.

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

RELATED DOCUMENTATION

show dot1x | 2644

Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

Example: Setting Up VoIP with 80.1X and LLDP-MED on an EX Series Switch | 528

Example: Configuring Static MAC Bypass of 80.1X and MAC RADIUS Authentication on an EX Series Switch | 479

Configuring 802.1X Interface Settings (CLI Procedure) | 390

Configuring 802.1X Authentication (J-Web Procedure)
disable (DNSSEC)

Syntax

disable;

Hierarchy Level

[edit system services dns dnssec]

Release Information
Statement introduced in Junos OS Release 10.2.

Description
Disables DNSSEC in the DNS server.

Required Privilege Level
system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

DHCP Overview | 909
disable (LLDP)

Syntax

disable;

Hierarchy Level

[edit protocols lldp],
[edit protocols interface lldp]

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

Description
Disable the LLDP configuration on the switch or on one or more interfaces.

Default
If you do not configure LLDP, it is disabled on the switch and on specific switch interfaces.

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

RELATED DOCUMENTATION

show lldp | 2680
Configuring LLDP (CLI Procedure) | 654
Understanding LLDP and LLDP-MED on EX Series Switches | 661
Understanding LLDP | 653
disable (LLDP-MED)

Syntax

disable;

Hierarchy Level

[edit protocols lldp-med],
[edit protocols lldp-med interface]

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

Description
Disable the LLDP-MED configuration on the switch or on one or more interfaces.

Default
If you do not configure LLDP-MED, it is disabled on the switch and on specific switch interfaces.

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

RELATED DOCUMENTATION

| show lldp | 2680 |
| Configuring LLDP (CLI Procedure) | 654 |
| Understanding LLDP and LLDP-MED on EX Series Switches | 661 |
**disable (LLDP Power Negotiation)**

**Syntax**

```disable;```

**Hierarchy Level**

```
[edit protocols lldp interface (all | interface-name) power-negotiation]
```

**Release Information**

Statement introduced in Junos OS Release 12.2 for EX Series switches.

**Description**

Disable Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE)-powered devices to allocate power.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring LLDP (CLI Procedure) | 654
- Configuring PoE on EX Series Switches (CLI Procedure)
disable-relay

Syntax

disable-relay;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface overrides]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Disable DHCP relay on specific interfaces in a group.

Required Privilege Level

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

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview | 792
dlv

Syntax

dlv {
    domain-name domain-name trusted-anchor trusted-anchor;
}

Hierarchy Level

[edit system services dns dnssec]

Release Information
Statement introduced in Junos OS Release 10.2.

Description
Configure DNSSEC Lookaside Validation (DLV).

Options
- domain-name domain-name—Specify the secure domain server name.
- trusted-anchor trusted-anchor—Specify the trusted DLV anchor.

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

RELATED DOCUMENTATION

| DHCP Overview | 909 |
domain (Domain Map)

Syntax

domain {
  delimiter [delimiter-character];
  map domain-map-name {
    aaa-logical-system logical-system-name {
      aaa-routing-instance routing-instance-name;
    }
    aaa-routing-instance routing-instance-name;
    access-profile profile-name;
    address-pool pool-name;
    dynamic-profile profile-name;
    padn destination-address {
      mask destination-mask;
      metric route-metric;
    }
    strip-domain;
    target-logical-system logical-system-name {
      target-routing-instance routing-instance-name;
    }
    target-routing-instance routing-instance-name;
    tunnel-profile profile-name;
  }
  parse-direction (left-to-right | right-to-left);
  parse-order (domain-first | realm-first);
  realm-delimiter [delimiter-character];
  realm-parse-direction (left-to-right | right-to-left);
}

Hierarchy Level

[edit access]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**RELATED DOCUMENTATION**

*Configuring a Domain Map*
domain-name (DHCP)

Syntax

```
domain-name domain-name;
```

Hierarchy Level

```
[edit system services dhcp]
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information

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

Description

Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.

Options

`domain-name`—Name of the domain.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring a DHCP Server on Switches (CLI Procedure) | 759
domain-name (DHCP Local Server)

Syntax

domain-name domain-name-string;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options
domain-name-string—Domain name formatted string.

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

RELATED DOCUMENTATION
| Using External AAA Authentication Services with DHCP | 833 |
domain-name (DHCP Relay Agent)

Syntax

domain-name domain-name-string;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description
Specify the domain name that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

*domain-name-string*—Domain name formatted string.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Using External AAA Authentication Services with DHCP | 833 |
| Creating Unique Usernames for DHCP Clients | 834 |
domain-name-server (Routing Instances and Access Profiles)

Syntax

```
domain-name-server dns-address;
```

Hierarchy Level

```
[edit access];
[edit access profile]
```

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is less preferred than one configured with the domain-name-server-inet statement. That is, the server with the address configured with the domain-name-server-inet takes precedence over a server configured with this statement.

Options

dns-address—IPv4 address of the DNS name server.

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

RELATED DOCUMENTATION

- Configuring DNS Name Server Addresses for Subscriber Management
- DNS Name Server Address Overview
domain-name-server-inet (Routing Instances and Access Profiles)

Syntax

domain-name-server-inet dns-address;

Hierarchy Level

[edit access], [edit access profile]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement. That is, the server with the address configured with the domain-name-server-inet takes precedence over a server configured with the domain-name-server statement.

Options

dns-address—IPv4 address of the DNS name server.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring DNS Name Server Addresses for Subscriber Management
DNS Name Server Address Overview
domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax

domain-name-server-inet6 dns-address;

Hierarchy Level

[edit access],
[edit access profile]

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

Options
dns-address—IPv6 address of the DNS name server.

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

RELATED DOCUMENTATION

Configuring DNS Name Server Addresses for Subscriber Management
DNS Name Server Address Overview
domain-search

Syntax

domain-search [domain-list ];

Hierarchy Level

[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

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

Description

Configure a list of domains to search (in the case where you want to configure access to multiple DNS servers for redundancy, and/or to resolve hosts that the previous server could not).

Options

domain-list—List of domain servers to search. The list can contain up to six domain names, separated by a space, with a total of up to 256 characters.

For example to search domain1.net, and if it fails to resolve the host, domain2.net, and if fails to resolve the host, domain3.net, you would configure the following domain list at the domain-search hierarchy level:

[edit system]
set domain-search [domain1.net domain2.net domain3.net]

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
dot1x

Syntax

dot1x {
    authenticator {
        authentication-profile-name access-profile-name;
        interface (all | [ interface-names ] | {
            disable;
            guest-vlan (vlan-id | vlan-name);
            lldp-med-bypass;
            mac-radius <restrict>;
            maximum-requests number;
            no-reauthentication;
            quiet-period seconds;
            reauthentication {
                interval seconds;
            }
            retries (802.1X) number;
            server-fail (deny | permit | use-cache | vlan-id | vlan-name);
            server-reject-vlan (vlan-id | vlan-name) {
                eapol-block;
                block-interval block-interval;
            }
            server-timeout seconds;
            supplicant (single | single-secure | multiple);
            supplicant-timeout seconds;
            transmit-period seconds;
        }
    }
    no-mac-table-binding;
    static mac-address {
        interface interface-names;
        vlan-assignment (vlan-id | vlan-name);
    }
}

Hierarchy Level

[edit protocols]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

**Description**
Configure 802.1X authentication for Port-Based Network Access Control. 802.1X authentication is supported on interfaces that are members of private VLANs (PVLANs).

The remaining statements are explained separately. See CLI Explorer.

**Default**
802.1X is disabled.

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

**RELATED DOCUMENTATION**

| show dot1x | 2644 |
| Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch | 440 |
| Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448 |
| Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528 |
| Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479 |
| Example: Configuring MAC RADIUS Authentication on an EX Series Switch | 427 |
| Configuring RADIUS Server Fail Fallback (CLI Procedure) | 384 |
drop (DHCP Relay Agent Option)

Syntax

drop;

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action | equals | starts-with)],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Drop (discard) specified DHCP client packets when you use DHCP relay agent selective processing. You can configure the drop operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Required Privilege Level

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

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic
dual-stack (DHCP Local Server Overrides)

Syntax

dual-stack dual-stack-group-name;

Hierarchy Level

[edit logical-systems name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems name system services dhcp-local-server ...],
[edit routing-instances name system services dhcp-local-server ...],
[edit system services dhcp-local-server group group-name interface interface-name overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server overrides]

Release Information
Statement introduced in Junos OS Release 17.3R1.

Description
Assigns the specified dual-stack group to both legs (DHCP and DHCPv6) of the DHCP dual stack. The dual-stack group defines the common configuration settings for DHCP and DHCPv6 subscribers on both legs. These settings take precedence over all other configurations, such as those specified in global, group, or interface settings.

Options

dual-stack-group-name—Name of the globally configured dual-stack group.

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

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview
Configuring Single-Session DHCP Dual-Stack Support
dual-stack (DHCP Relay Agent Overrides)

Syntax

dual-stack dual-stack-group-name;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 15.1.

Description
Assigns the specified dual-stack group to both legs (DHCP and DHCPv6) of the DHCP dual stack. The dual-stack group defines the common configuration settings for DHCP and DHCPv6 subscribers on both legs. These settings take precedence over all other configurations, such as those specified in global, group, or interface settings.

Options
dual-stack-group-name—Name of the globally configured dual-stack group.

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Single-Session DHCP Dual-Stack Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Single-Session DHCP Dual-Stack Support</td>
</tr>
</tbody>
</table>
dual-stack-group (DHCP Local Server)

Syntax

dual-stack-group name {
    access-profile access-profile;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    classification-key {
        circuit-id circuit-id;
        mac-address mac-address;
        remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    on-demand-address-allocation;
    protocol-master (inet | inet6);
}
reauthenticate {<lease-renewal> <remote-id-mismatch >};
  service-profile service-profile;
  short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}

Hierarchy Level
[edit logical-systems name routing-instances name system services dhcp-local-server],
[edit logical-systems name system services dhcp-local-server],
[edit routing-instances name system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information
Statement introduced in Junos OS Release 17.3R1 on MX Series routers.

Description
Specifies common configuration settings that are used for both legs (DHCP and DHCPv6) of the DHCP local server dual-stack, and names the dual-stack group.

When applied, the dual-stack configuration takes precedence over all other configurations, such as those specified in global, group, or interface settings.

Options
name—Name of the dual-stack group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview
DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 873
Configuring RADIUS Reauthentication for DHCP Subscribers
RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers
dual-stack-group (DHCP Relay Agent)

Syntax

dual-stack-group name {
  access-profile profile-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name delimiter-character;
      interface-description (device-interface | logical-interface);
      interface-name;
      logical-system-name;
      mac-address;
      relay-agent-interface-id;
      relay-agent-remote-id;
      routing-instance-name;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
  }
  dual-stack-interface-client-limit number;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
      layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
      }
    }
  }
  protocol-master (inet | inet6);
  relay-agent-interface-id {

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]

Release Information
Statement introduced in Junos OS Release 15.1.

Description
Specifies common configuration settings that are used for both legs (DHCP and DHCPv6) of the DHCP dual stack, and names the dual stack group.

The group is assigned to each leg of the DHCP dual-stack with the dual-stack statement in the overrides stanza. When applied, the dual-stack configuration takes precedence over all other configurations, such as those specified in global, group, or interface settings.

Options
name—Name of the dual-stack group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement in the configuration.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview
Configuring Single-Session DHCP Dual-Stack Support
DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 873
dual-stack-interface-client-limit (DHCP Local Server and Relay Agent)

Syntax

dual-stack-interface-client-limit number;

Hierarchy Level

[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit system services dhcp dhcp-local-server dual-stack-group dual-stack-group-name ],

Release Information

Statement introduced in Junos OS Release 17.3R1.

Description

Limit the number of clients allowed on an interface.

Options

number—Maximum number of dual-stack subscribers that can log in per interface.

Range: 1 through 500,000

Required Privilege Level

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

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview
duplication (Access Profile)

Syntax

duplication;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Configure the router to send accounting reports to both the RADIUS accounting server configured in the access profile for the wholesaler and the RADIUS accounting server configured in the access profile for the retailer.

Default
The router sends accounting reports to the accounting servers that are in the context in which the subscriber is authenticated.

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

RELATED DOCUMENTATION

Configuring Authentication and Accounting Parameters for Subscriber Access
Understanding RADIUS Accounting Duplicate Reporting
duplication-filter (Access Profile)

**Syntax**

duplication-filter (interim-duplicated | interim-original) <exclude-attributes>;

**Hierarchy Level**

[edit access profile profile-name accounting]

**Release Information**


**Description**
Configure which accounting servers receive accounting messages when RADIUS duplication accounting is configured in the access profile.

**Options**

- **exclude-attributes**—(Optional) Filter RADIUS attributes from duplicated accounting interim messages based on the exclude statement configuration in the corresponding duplication access profile. You can configure exclude-attributes alone, or with interim-duplicated or interim-original.

- **interim-duplicated**—Do not send accounting interim messages to RADIUS accounting servers that are in a duplication context other than the subscriber's access profile.

- **interim-original**—Do not send accounting interim messages to RADIUS accounting servers that are in the subscriber's access profile.

**NOTE:** The interim-duplicated and interim-original filters are mutually exclusive.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Understanding RADIUS Accounting Duplicate Reporting
duplication-vrf (Duplicate Accounting)

Syntax

duplication-vrf {
    access-profile-name profile-name;
    vrf-name vrf-name;
}

Hierarchy Level

[edit access profile profile-name accounting]

Release Information
Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description
Configure the router to send duplicate accounting information to the RADIUS accounting servers defined in up to five access profiles all in the same nondefault VRF (LS:RI combination).

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

Understanding RADIUS Accounting Duplicate Reporting
Configuring Authentication and Accounting Parameters for Subscriber Access
**dynamic-pool**

**Syntax**

```
dynamic-pool <dynamic-pool>
family {
    inet6 {
        from-interface <interface>;
        delegated-prefix-length <network-prefix-length>;
        range <range-name> {
            masked-low <masked-low>;
            masked-high <masked-high>;
            prefix-length <prefix-length>;
        }
        dhcp-attributes {
            dns-server <address>;
            t1-percentage <t1-percentage>;
            t2-percentage <t2-percentage>;
            preferred-lifetime <preferred-lifetime>;
            valid-lifetime <valid-lifetime>;
        }
    }
}
```

**Hierarchy Level**

[edit access address-assignment (Access)]

**Release Information**

Statement introduced in Junos OS Release 15.1X49-D70.

**Description**

Configure the dynamic pool updated by the client running on the WAN interface.

**Options**

The remaining statements are explained separately.

**Required Privilege Level**

access—To view this statement in the configuration.
access-control—To add this statement to the configuration.
RELATED DOCUMENTATION

Configuring Address-Assignment Pools | 929

address-assignment (Access) | 1475
dynamic-profile (DHCP Local Server)

Syntax

dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options aggregate-clients and use-primary introduced in Junos OS Release 9.3.
Support at the [edit ... interface] hierarchy levels introduced in Junos OS Release 11.2.

Description

Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.

Options

profile-name—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

- Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
- Configuring a Default Subscriber Service
dynamic-profile (DHCP Relay Agent)

Syntax

```
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
```

Hierarchy Level

- `[edit forwarding-options dhcp-relay]`
- `[edit forwarding-options dhcp-relay dhcpv6]`
- `[edit forwarding-options dhcp-relay dhcpv6 group group-name]`
- `[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]`
- `[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name]`
- `[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name]`
- `[edit forwarding-options dhcp-relay group group-name]`
- `[edit forwarding-options dhcp-relay group group-name interface interface-name]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay ...]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]`

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support at the `[edit ... dual-stack-group dual-stack-group-name]` hierarchy level introduced in Junos OS Release 15.1.

Description

Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.

M120 and M320 routers do not support DHCPv6.

Options

- `profile-name`—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

dhcp-relay | 1665

| Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces |
| Grouping Interfaces with Common DHCP Configurations | 853 |
| Configuring a Default Subscriber Service |

dynamic-profile-options

Syntax

dynamic-profile-options {
    versioning;
}

Hierarchy Level

[edit system]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Configure global dynamic profile options.

The remaining statement is explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

| Versioning for Dynamic Profiles |
dynamic-server

Syntax

dhcpv6 {
dynamic-server {
group <group> {
neighbor-discovery-router-advertisement <ndra-pool>;
interface <interface> {
overrides {
   delegated-pool <delegated-pool>;
ia-na-pool <ia-na-pool>;
process-inform {
pool <pool>;
}
}
}
}
}
}

Hierarchy Level
[edit system services]

Release Information
Statement introduced in Junos OS Release 15.1X49-D70.

Description
Configure the server running on a LAN interface.

Options
The remaining statements are explained separately.

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

RELATED DOCUMENTATION
dhcp-local-server (System Services) | 1660
dhcp-client | 1641
**eapol-block**

**Syntax**

```plaintext
eapol-block {
    server-fail {
        seconds;
    }
    mac-radius;
    captive-portal;
}
```

**Hierarchy Level**

```
[edit protocols dot1x authenticator interface (interface-names)],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan],
[edit protocols dot1x authenticator interface (all | [interface-names]) server-reject-vlan (vlan-id | vlan-name)]
```

**Release Information**

Statement introduced in Junos OS Release 11.2 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Support at the [edit protocols dot1x authenticator interface interface-name] hierarchy level introduced in Junos OS Releases 14.1X53-D40 and 15.1X53-D51 for EX Series switches.
Support for options mac-radius and captive-portal introduced in Junos OS Release 17.2R1.

**Description**

Enable the switch to ignore Extensible Authentication Protocol over LAN (EAPoL)-Start messages received from a client that has been authenticated so that the switch does not trigger re-authentication. The switch typically attempts to restart the authentication procedure by contacting the authentication server when it receives an EAPoL-Start message from a client—even for authenticated clients. You can configure the eapol-block statement to help prevent unnecessary downtime that can occur when the switch waits for a response from the authentication server.

If you configure the switch to block EAPoL-Start messages, when the switch receives an EAPoL-Start message from an authenticated client, the switch ignores the message and does not attempt to contact the authentication server for reauthentication. The existing authentication session that was established for the client remains open.

The EAPoL-Start messages are blocked only if the client is in the authenticated state. EAPoL-Start messages from new clients are accepted.

**Default**
If the `eapol-block` statement is not configured, the switch attempts to contact the authentication server to authenticate the client when it receives an EAPoL-Start message.

**Options**

`server-fail seconds`—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using server fail fallback or server reject VLAN methods. Configure the time interval, in seconds, during which the switch will not attempt to contact the authentication server to re-authenticate a client that has already been authenticated using server fail fallback.

**Default:** 120 seconds.

**Range:** 120 through 65,535 seconds.

`mac-radius (EX4300 and EX9200 switches only)`—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using MAC RADIUS authentication. The `mac-radius` option is also valid for clients authenticated using central Web authentication (CWA).

`captive-portal (EX4300 and EX9200 switches only)`—Configure the switch to ignore EAP-Start messages received from a client that has been authenticated using captive portal authentication.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>block-interval</th>
<th>1537</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients</td>
<td>415</td>
</tr>
</tbody>
</table>
elin

Syntax

elin number;

Hierarchy Level

[edit protocols lldp-med interface (all | interface-name location)]

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the Emergency Line Identification Number (ELIN) as location information. Location information is advertised from the switch to the MED device and is used during emergency calls to identify the location of the MED device.

Default

Disabled.

Options

number—Configure a 10-digit number (area code and telephone number).

Required Privilege Level

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

RELATED DOCUMENTATION

| show lldp | 2680 |
| Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528 |
| Configuring LLDP-MED (CLI Procedure) | 665 |
encoding

Syntax

encoding (binary | pem);

Hierarchy Level

[edit security ike policy ike-peer-address],
[edit security certificates certification-authority ca-profile-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the local-certificate and local-key-pair statements.

Options
binary—Binary file format.
pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.

Default: binary

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

RELATED DOCUMENTATION

Configuring the Type of Encoding Your CA Supports
Configuring an IKE Policy for Digital Certificates for an ES PIC
enhanced-accounting

Syntax

enhanced-accounting;

Hierarchy Level

[edit system radius-options]
[edit system tacplus-options],

Release Information

Description
Configure audit of TACACS+ or RADIUS authentication events such as access method, remote port, and access privileges.

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

RELATED DOCUMENTATION

| radius-options | 2144 |
| tacplus-options | 2308 |
| Configuring RADIUS System Accounting | 255 |
| Configuring TACACS+ System Accounting | 278 |
enhanced-avs-max

Syntax

```
enhanced-avs-max <number>;
```

Hierarchy Level

```
[edit system accounting]
```

Release Information


Description

Configure the number of attribute values to be displayed.

Options

```
<number>—Number of attribute values.
```

Range: 7 through 15

Default: 7

Required Privilege Level

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>documentation</th>
<th>page</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>1455</td>
</tr>
<tr>
<td>enhanced-accounting</td>
<td>1756</td>
</tr>
<tr>
<td>Configuring RADIUS System Accounting</td>
<td>255</td>
</tr>
<tr>
<td>Configuring TACACS+ System Accounting</td>
<td>278</td>
</tr>
</tbody>
</table>
enrollment-retry

Syntax

enrollment-retry attempts;

Hierarchy Level

[edit security certificates]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

Options
attempts—Number of enrollment retries.

Range: 0 through 100
Default: 0

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

RELATED DOCUMENTATION

Configuring the Number of Enrollment Retries
**enrollment-url**

**Syntax**

```
enrollment-url url-name;
```

**Hierarchy Level**

```
[edit security certificates certification-authority ca-profile-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

(Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

**Options**

`url-name`—Certificate authority URL.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

*Specifying an Enrollment URL*
List of Syntax

EX Series on page 1760
QFX Series, QFabric, EX4600 on page 1765

ethernet-switching-options

```
ethernet-switching-options {
    analyzer (Port Mirroring) {
        name {
            loss-priority priority;
            ratio number;
            input {
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
                egress {
                    interface (all | interface-name);
                }
            }
            output {
                interface interface-name;
                vlan (vlan-id | vlan-name) {
                    no-tag;
                }
            }
        }
    }
    bpdu-block {
        disable-timeout timeout;
        interface (all | interface-name) {
            {disable | drop | shutdown};
        }
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100);
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-lookup-length number-of-entries;
}
```
mac-notification {
    notification-interval seconds;
}
mac-table-aging-time seconds;
nonstop-bridging;
port-error-disable {
    disable-timeout timeout;
}
redundant-trunk-group {
    group name {
        interface interface-name <primary>;
        interface interface-name;
    }
}
secure-access-port {
    dhcp-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    dhcpv6-snooping-file {
        location local_pathname | remote_URL;
        timeout seconds;
        write-interval seconds;
    }
    interface (all | interface-name) {
        allowed-mac {
            mac-address-list;
        }
        (dhcp-trusted | no-dhcp-trusted);
        fcoe-trusted;
        mac-limit limit action (drop | log | none | shutdown);
        no-allowed-mac-log;
        persistent-learning;
        static-ip ip-address {
            vlan vlan-name;
            mac mac-address;
        }
        static-ipv6 ip-address {
            vlan vlan-name;
            mac mac-address;
        }
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection) {
            forwarding-class class-name;
        }
    }
    dhcp-option82 {
        circuit-id {
            prefix hostname;
            use-interface-description;
            use-vlan-id;
        }
        remote-id {
            prefix hostname | mac | none;
            use-interface-description;
            use-string string;
        }
    }
vendor-id [string];

(examine-dhcp | no-examine-dhcp) {
    forwarding-class class-name;
}

(examine-dhcpv6 | no-examine-dhcpv6) {
    forwarding-class class-name;
}

(examine-fip {
    fc-map fc-map-value;
})

(ip-source-guard | no-ip-source-guard);
(ipv6-source-guard | no-ipv6-source-guard);
mac-move-limit limit action (drop | log | none | shutdown);

(neighbor-discovery-inspection | no-neighbor-discovery-inspection);

no-option-37;

static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}

storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        level level;
        multicast;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}

traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag flag <disable>;
}
unknown-unicast-forwarding {
    vlan (all | vlan-name) {
        interface interface-name;
    }
}

voip {
    interface (all | [interface-name | access-ports]) {
        vlan vlan-name;
        forwarding-class (assured-forwarding | best-effort | expedited-forwarding | network-control);
    }
}
}
QFX Series, QFabric, EX4600

ethernet-switching-options {
    analyzer {
        name {
            input {
                egress {
                    interface (all | interface-name);
                }
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
            }
            output {
                interface interface-name;
                ip-address ip-address;
                vlan (vlan-id | vlan-name);
            }
        }
        bpdu-block {
            interface (all | [interface-name]);
            disable-timeout timeout;
        }
        dot1q-tunneling {
            ether-type (0x8100 | 0x88a8 | 0x9100)
        }
        interfaces interface-name {
            no-mac-learning;
        }
        mac-table-aging-time seconds {
        }
        port-error-disable {
            disable-timeout timeout;
        }
        secure-access-port {
            dhcp-snooping-file {
                location local_pathname | remote_URL;
                timeout seconds;
                write-interval seconds;
            }
            interface (all | interface-name) {
                allowed-mac {
                    mac-address-list;
                }
            }
        }
    }
}
(dhcp-trusted | no-dhcp-trusted);
fcoe-trusted;
mac-limit limit action action;
no-allowed-mac-log;
}

vlan (all | vlan-name) {
  (arp-inspection | no-arp-inspection) [
    forwarding-class (for DHCP Snooping or DAI Packets) class-name;
  ]
}
dhcp-option82 {
  circuit-id {
    prefix (Circuit ID for Option 82) hostname;
    use-interface-description;
    use-vlan-id;
  }
  remote-id {
    prefix (Remote ID for Option 82) hostname | mac | none;
    use-interface-description;
    use-string string;
  }
  vendor-id <string>;
}

(examine-dhcp | no-examine-dhcp) {
  forwarding-class (for DHCP Snooping or DAI Packets) class-name;
}

examine-fip {
  examine-vn2vn {
    beacon-period milliseconds;
  }
  fc-map fc-map-value;
}

mac-move-limit limit <fabric-limit limit action action;
storm-control {  
  interface (all | interface-name) {  
    bandwidth bandwidth;  
    no-broadcast;  
    no-multicast;  
    no-unknown-unicast;  
  }  
}  
}  
traceoptions {  
  file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;  
  flag flag <disable>;  
}  
}

Hierarchy Level

[edit]

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

Description
Configure Ethernet switching options.

The remaining statements are explained separately. See CLI Explorer.

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

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Port Mirroring</td>
<td></td>
</tr>
<tr>
<td>Understanding How to Protect Access Ports from Common Attacks</td>
<td></td>
</tr>
<tr>
<td>Port Security Features</td>
<td></td>
</tr>
<tr>
<td>Understanding BPDU Protection for STP, RSTP, and MSTP</td>
<td></td>
</tr>
<tr>
<td>Understanding Redundant Trunk Links (Legacy RTG Configuration)</td>
<td></td>
</tr>
<tr>
<td>Understanding Storm Control</td>
<td></td>
</tr>
<tr>
<td>Understanding 802.1X and VoIP on EX Series Switches</td>
<td>525</td>
</tr>
<tr>
<td>Understanding Q-in-Q Tunneling and VLAN Translation</td>
<td></td>
</tr>
<tr>
<td>Understanding and Preventing Unknown Unicast Forwarding</td>
<td></td>
</tr>
<tr>
<td>Understanding MAC Notification on EX Series Switches</td>
<td></td>
</tr>
<tr>
<td>Understanding FIP Snooping</td>
<td></td>
</tr>
<tr>
<td>Understanding Nonstop Bridging on EX Series Switches</td>
<td></td>
</tr>
</tbody>
</table>
events

Syntax

```
events (change-log | interactive-commands | login);
```

Hierarchy Level

```
[edit system accounting]
```

Release Information

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

Description

Configure the types of events to track and log.

Options

- `change-log`—Audit configuration changes.
- `interactive-commands`—Audit interactive commands (any command-line input).
- `login`—Audit logins.

Required Privilege Level

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

RELATED DOCUMENTATION

- Specifying TACACS+ Auditing and Accounting Events | 279
- Configuring RADIUS System Accounting | 255
exclude (RADIUS Attributes)

Syntax

```
exclude {
  acc-aggr-cir-id-asc [ access-request | accounting-start | accounting-stop ];
  acc-aggr-cir-id-bin [ access-request | accounting-start | accounting-stop ];
  acc-loop-cir-id [ access-request | accounting-start | accounting-stop ];
  acc-loop-encap [ access-request | accounting-start | accounting-stop ];
  acc-loop-remote-id [ access-request | accounting-start | accounting-stop ];
  accounting-session-id access-request;
  accounting-terminate-cause accounting-off;
  acct-request-reason [ accounting-start | accounting-stop ];
  acct-tunnel-connection [ access-request | accounting-start | accounting-stop ];
  act-data-rate-dn [ access-request | accounting-start | accounting-stop ];
  act-data-rate-up [ access-request | accounting-start | accounting-stop ];
  act-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
  act-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
  att-data-rate-dn [ access-request | accounting-start | accounting-stop ];
  att-data-rate-up [ access-request | accounting-start | accounting-stop ];
  called-station-id [ access-request | accounting-start | accounting-stop ];
  calling-station-id [ access-request | accounting-start | accounting-stop ];
  chargeable-user-identity access-request;
  class [ accounting-start | accounting-stop ];
  cos-shaping-rate [ accounting-start | accounting-stop ];
  delegated-ipv6-prefix [ accounting-start | accounting-stop ];
  dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
  dhcp-header access-request;
  dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
  dhcp-options [ access-request | accounting-start | accounting-stop ];
  dhcpv6-header access-request;
  dhcpv6-options [ access-request | accounting-start | accounting-stop ];
  downstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
  dsl-forum-attributes [ access-request | accounting-start | accounting-stop ];
  dsl-line-state [ access-request | accounting-start | accounting-stop ];
  dsl-type [ access-request | accounting-start | accounting-stop ];
  dynamic-ifset-name [ accounting-start | accounting-stop ];
  event-timestamp [ accounting-off | accounting-on | accounting-start | accounting-stop ];
  filter-id [ accounting-start | accounting-stop ];
  first-relay-ipv4-address [ access-request | accounting-start | accounting-stop ];
  first-relay-ipv6-address [ access-request | accounting-start | accounting-stop ];
  framed-interface-id [ access-request | accounting-start | accounting-stop ];
```
framed-ip-address [ access-request | accounting-start | accounting-stop ];
framed-ip-netmask [ access-request | accounting-start | accounting-stop ];
framed-ip-route [ accounting-start | accounting-stop ];
framed-ipv6-address [ access-request | accounting-start | accounting-stop ];
framed-ipv6-pool [ accounting-start | accounting-stop ];
framed-ipv6-prefix [ accounting-start | accounting-stop ];
framed-ipv6-route [ accounting-start | accounting-stop ];
framed-pool [ accounting-start | accounting-stop ]; input-ipv6-gigawords accounting-stop;
input-filter [ accounting-start | accounting-stop ];
in-gigapackets accounting-stop;
in-gigawords accounting-stop;
in-ipv6-octets accounting-stop;
in-ipv6-packets accounting-stop;
in interface-description [ access-request | accounting-start | accounting-stop ];
l2c-downstream-data [ access-request | accounting-start | accounting-stop ];
l2c-upstream-data [ access-request | accounting-start | accounting-stop ];
l2tp-rx-connect-speed [ access-request | accounting-start | accounting-stop ];
l2tp-tx-connect-speed [ access-request | accounting-start | accounting-stop ];
max-data-rate-dn [ access-request | accounting-start | accounting-stop ];
max-data-rate-up [ access-request | accounting-start | accounting-stop ];
max-interlv-delay-dn [ access-request | accounting-start | accounting-stop ];
max-interlv-delay-up [ access-request | accounting-start | accounting-stop ];
min-data-rate-dn [ access-request | accounting-start | accounting-stop ];
min-data-rate-up [ access-request | accounting-start | accounting-stop ];
min-lp-data-rate-dn [ access-request | accounting-start | accounting-stop ];
min-lp-data-rate-up [ access-request | accounting-start | accounting-stop ];
nas-identifier [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
nas-port [ access-request | accounting-start | accounting-stop ];
nas-port-id [ access-request | accounting-start | accounting-stop ];
nas-port-type [ access-request | accounting-start | accounting-stop ];
output-filter [ accounting-start | accounting-stop ];
output-gigapackets accounting-stop;
output-gigawords accounting-stop;
output-ipv6-gigawords accounting-stop;
output-ipv6-octets accounting-stop;
output-ipv6-packets accounting-stop;
pppoe-description [ access-request | accounting-start | accounting-stop ];
standard-attribute number {
    packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
}
tunnel-assigment-id [ access-request | accounting-start | accounting-stop ];
tunnel-client-auth-id [ access-request | accounting-start | accounting-stop ];
tunnel-client-endpoint [ access-request | accounting-start | accounting-stop ];
tunnel-medium-type [ access-request | accounting-start | accounting-stop ];
tunnel-server-auth-id [ access-request | accounting-start | accounting-stop ];
tunnel-server-endpoint [ access-request | accounting-start | accounting-stop ];
tunnel-type [ access-request | accounting-start | accounting-stop ];
upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
vendor-id id-number {
    vendor-attribute vsa-number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
    }
}
virtual-router [ access-request | accounting-start | accounting-stop ];
}

Hierarchy Level

[edit access profile profile-name radius attributes]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
downstream-calculated-qos-rate, dsl-forum-attributes, and upstream-calculated-qos-rate options added in Junos OS Release 11.4.
cos-shaping-rate and filter-id options added in Junos OS Release 13.2.
pppoe-description option added in Junos OS Release 14.2.
virtual-router option added in Junos OS Release 15.1.
first-relay-ipv4-address and first-relay-ipv6-address options added in Junos OS Release 16.1.
acc-loop-encap and acc-loop-remote-id options added in Junos OS Release 16.1R4.
access-request option support for all tunnel attributes added in Junos OS Release 15.1R7, 16.1R5, 16.2R2, 17.1R2, 17.2R2, and 17.3R1 for MX Series.
packet-type, standard-attribute, vendor-attribute, and vendor-id options added in Junos OS Release 18.1R1.
Description

Configure the router or switch to exclude the specified attributes from being sent in the specified type of RADIUS message. Exclusion can be useful, for example, for attributes that do not change values over the lifetime of a subscriber. By not sending these attributes, you reduce the packet size without losing information. Contrast this behavior with that provided by the ignore statement.

You can specify attribute exclusion for multiple RADIUS message types by enclosing the message types, separated by spaces, within brackets ([ ]). You do not need brackets when specifying a single message type.

Starting in Junos OS Release 18.1R1, you can specify standard RADIUS attributes with the attribute number. You can specify VSAs with the IANA-assigned vendor ID and the VSA number. With this flexible configuration method, you can configure any standard attribute and VSA supported by your platform to be excluded. The configuration has no effect if you configure unsupported attributes, vendors, and VSAs.

The legacy method allows you to configure only those attributes and VSAs for which the statement syntax includes a specific option. Consequently, you can use the legacy method to exclude only a subset of all attributes that can be received in Access-Accept messages.

Not all attributes are available in all types of RADIUS messages.

**NOTE:** If you exclude an attribute from Acct-Off messages, the attributes are then excluded from Interim-Acct messages.

**NOTE:** VSAs with dedicated option names include Juniper Networks (IANA vendor ID 4874) and DSL Forum (vendor ID 3561) VSAs.
Options

RADIUS attribute—RADIUS standard attribute or VSA:

- **acc-aggr-cir-id-asc**—Exclude Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **acc-aggr-cir-id-bin**—Exclude Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
- **acc-loop-cir-id**—Exclude Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
- **acc-loop-encap**—Exclude Juniper Networks VSA 26-183, Acc-Loop-Encap.
- **acc-loop-remote-id**—Exclude Juniper Networks VSA 26-182, Acc-Loop-Remote-Id.
- **accounting-authentic**—Exclude RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—Exclude RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—Exclude RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—Exclude RADIUS attribute 49, Acct-Terminate-Cause.
- **acct-request-reason**—Exclude Juniper Networks VSA 26-210, Acct-Request-Reason.
- **acct-tunnel-connection**—Exclude RADIUS attribute 68, Acct-Tunnel-Connection.
- **act-data-rate-dn**—Exclude Juniper Networks VSA 26-114, Act-Data-Rate-Dn.
- **act-data-rate-up**—Exclude Juniper Networks VSA 26-113, Act-Data-Rate-Up.
- **act-interlv-delay-dn**—Exclude Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn.
- **att-data-rate-dn**—Exclude Juniper Networks VSA 26-118, Att-Data-Rate-Dn.
- **att-data-rate-up**—Exclude Juniper Networks VSA 26-117, Att-Data-Rate-Up.
- **called-station-id**—Exclude RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—Exclude RADIUS attribute 31, Calling-Station-Id.
- **chargeable-user-identity**—Exclude RADIUS attribute 89, Chargeable-User-Identity.
- **class**—Exclude RADIUS attribute 25, Class.
- **cos-shaping-rate**—Exclude Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **delegated-ipv6-prefix**—Exclude RADIUS attribute 123, Delegated-Ipv6-Prefix.
- **dhcp-gi-address**—Exclude Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-header**—Exclude Juniper Networks VSA 26-208, DHCP-Header.
- **dhcp-mac-address**—Exclude Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Exclude Juniper Networks VSA 26-55, DHCP-Options.
- **dhcpv6-header**—Exclude Juniper Networks VSA 26-209, DHCPv6-Header.
- **dhcpv6-options**—Exclude Juniper Networks VSA 26-207, DHCPv6-Options.
- **dynamic-ifiset-name**—Exclude Juniper Networks VSA 26-130, Qos-Set-Name.
- **downstream-calculated-qos-rate**—Exclude Juniper Networks VSA 26-141.
- **dsl-forum-attributes**—Exclude DSL Forum VSA (vendor ID 3561) as described in RFC 4679, DSL Forum Vendor-Specific RADIUS Attributes.
- **dsl-line-state**—Exclude Juniper Networks VSA 26-127, DSL-Line-State.
- **dsl-type**—Exclude Juniper Networks VSA 26-128, DSL-Type.
- **event-timestamp**—Exclude RADIUS attribute 55, Event-Timestamp.
- **filter-id**—Exclude RADIUS attribute 11, Filter-Id.
- **first-relay-ipv4-address**—Exclude Juniper Networks VSA 26-189, DHCP-First-Relay-IpV4-Address.
- **first-relay-ipv6-address**—Exclude Juniper Networks VSA 26-190, DHCP-First-Relay-IpV6-Address.
- **framed-interface-id**—Exclude RADIUS attribute 96, Framed-Interface-ID.
- **framed-ip-address**—Exclude RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—Exclude RADIUS attribute 9, Framed-IP-Netmask.
- **framed-ip-route**—Exclude RADIUS attribute 22, Framed-Route.
- **framed-ipv6-address**—Exclude RADIUS attribute 168, Framed-IPv6-Address.
- **framed-ipv6-pool**—Exclude RADIUS attribute 100, Framed-IPv6-Pool.
- **framed-ipv6-prefix**—Exclude RADIUS attribute 97, Framed-IPv6-Prefix.
- **framed-ipv6-route**—Exclude RADIUS attribute 99, Framed-IPv6-Route.
- **framed-pool**—Exclude RADIUS attribute 88, Framed-Pool.
- **input-filter**—Exclude Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Exclude Juniper Networks VSA 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—Exclude RADIUS attribute 52, Acct-Input-Gigawords.
- **input-ipv6-gigawords**—Exclude Juniper Networks VSA 26-155, Acct-Input-IpV6-Gigawords.
- **input-ipv6-octets**—Exclude Juniper Networks VSA 26-151, Acct-Input-IpV6-Octets.
- **input-ipv6-packets**—Exclude Juniper Networks VSA 26-153, Acct-Input-IpV6-Packets.
- **interface-description**—Exclude Juniper Networks VSA 26-53, Interface-Desc.
- **l2c-downstream-data**—Exclude Juniper Networks VSA 26-93, L2C-Down-Stream-Data.
- **l2c-upstream-data**—Exclude Juniper Networks VSA 26-92, L2C-Up-Stream-Data.
- **l2tp-rx-connect-speed**—Exclude Juniper Networks VSA 26-163, Rx-Connect-Speed.
- **l2tp-tx-connect-speed**—Exclude Juniper Networks VSA 26-162, Tx-Connect-Speed.
- **max-data-rate-dn**—Exclude Juniper Networks VSA 26-120, Max-Data-Rate-Dn.
• **max-data-rate-up**—Exclude Juniper Networks VSA 26-119, Max-Data-Rate-Up.
• **max-interlv-delay-dn**—Exclude Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn.
• **max-interlv-delay-up**—Exclude Juniper Networks VSA 26-123, Max-Interlv-Delay-Up.
• **min-data-rate-dn**—Exclude Juniper Networks VSA 26-116, Min-Data-Rate-Dn.
• **min-data-rate-up**—Exclude Juniper Networks VSA 26-115, Min-Data-Rate-Up.
• **min-lp-data-rate-dn**—Exclude Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn.
• **min-lp-data-rate-up**—Exclude Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up.
• **nas-identifier**—Exclude RADIUS attribute 32, NAS-Identifier.
• **nas-port**—Exclude RADIUS attribute 5, NAS-Port.
• **nas-port-id**—Exclude RADIUS attribute 87, NAS-Port-Id.
• **nas-port-type**—Exclude RADIUS attribute 61, NAS-Port-Type.
• **output-filter**—Exclude Juniper Networks VSA 26-11, Egress-Policy-Name.
• **output-gigapackets**—Exclude Juniper Networks VSA 26-43, Acct-Output-Gigapackets.
• **output-gigawords**—Exclude RADIUS attribute 53, Acct-Output-Gigawords.
• **output-ipv6-gigawords**—Exclude Juniper Networks VSA 26-156, Acct-Output-IPv6-Gigawords.
• **output-ipv6-octets**—Exclude Juniper Networks VSA 26-152, Acct-Output-IPv6-Octets.
• **output-ipv6-packets**—Exclude Juniper Networks VSA 26-154, Acct-Output-IPv6-Packets.
• **packet-type**—Specify the RADIUS message type to exclude; term required when excluding a standard attribute or VSA by number rather than name. You can enclose multiple values in square brackets to specify a list of message types. Message types include Access-Request, Accounting-Off, Accounting-Off, Accounting-Start, and Accounting-Stop.
• **pppoe-description**—Exclude Juniper Networks VSA 26-24, PPPoE-Description.
• **standard-attribute number**—RADIUS standard attribute number supported by your platform. If you configure an unsupported attribute, that configuration has no effect. When you use this option, you must use the **packet-type** term to specify the message from which the attribute is excluded.
• **tunnel-assignment-id**—Exclude RADIUS attribute 82, Tunnel-Assignment-ID.
• **tunnel-client-auth-id**—Exclude RADIUS attribute 90, Tunnel-Client-Auth-ID.
• **tunnel-client-endpoint**—Exclude RADIUS attribute 66, Tunnel-Client-Endpoint.
• **tunnel-medium-type**—Exclude RADIUS attribute 65, Tunnel-Medium-Type.
• **tunnel-server-auth-id**—Exclude RADIUS attribute 91, Tunnel-Server-Auth-ID.
• **tunnel-server-endpoint**—Exclude RADIUS attribute 67, Tunnel-Server-Endpoint.
• **tunnel-type**—Exclude RADIUS attribute 64, Tunnel-Type.
• **upstream-calculated-qos-rate**—Exclude Juniper Networks VSA 26-142

• **vendor-attribute vsa-number**—Number identifying a VSA belonging to the specified vendor; both must be supported by your platform. If you configure an unsupported VSA, that configuration has no effect. When you use this option, you must use the **packet-type** term to specify the message from which the attribute is excluded.

• **vendor-id id-number**—IANA vendor ID supported by your platform. If you configure an unsupported vendor ID, that configuration has no effect.

• **virtual-router**—Exclude Juniper Networks VSA 26-1.

RADIUS message type:

• **access-request**—RADIUS Access-Request messages.

• **accounting-off**—RADIUS Accounting-Off messages.

• **accounting-on**—RADIUS Accounting-On messages.

• **accounting-start**—RADIUS Accounting-Start messages.

• **accounting-stop**—RADIUS Accounting-Stop messages.

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

**RELATED DOCUMENTATION**

*Filtering RADIUS Attributes and VSAs from RADIUS Messages*

*RADIUS Servers and Parameters for Subscriber Access*

*Standard and Vendor-Specific RADIUS Attributes*
excluded-address (Address-Assignment Pools)

Syntax

excluded-address ip-address;

Hierarchy Level

[edit access addressassignment-addresspool]

Release Information
Statement introduced in Junos OS Release 15.1X49-D20.

Description
Allows you to exclude select IPv4 or IPv6 addresses from a DHCP address pool. Within a configured address pool, you can specifically exclude up to 20 addresses. Junos OS will not assign these excluded addresses to any clients. If you configure an excluded address that has already been assigned to a DHCP client, that excluded address will be revoked from the client.

NOTE: Excluded addresses must match the address family of the configured address pool. For example, you cannot exclude an IPv4 address within an IPv6 address pool.

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

RELATED DOCUMENTATION

pool

Preventing Addresses from Being Allocated from an Address Pool
excluded-address (Address-Assignment Pools)

Syntax

```
excluded-address ip-address;
```

Hierarchy Level

```
[edit access address-assignment pool name family (inet | inet6)],
[edit logical-systems name access address-assignment pool name family (inet | inet6)],
[edit logical-systems name routing-instances name access address-assignment pool name family (inet | inet6)],
[edit routing-instances name access address-assignment pool name family (inet | inet6)]
```

Release Information

Statement introduced in Junos OS Release 18.1R1 on MX Series routers.

Description

Specify an address to exclude from consideration when addresses are allocated from the corresponding address pool. If an address that you configure for exclusion has already been allocated, the subscriber that has that address is logged out. The address is then deallocated and marked for exclusion from future allocation.

Options

`ip-address`—IPv4 or IPv6 address to exclude from the address pool for the specified family.

Required Privilege Level

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

RELATED DOCUMENTATION

- Preventing Addresses from Being Allocated from an Address Pool
- Address-Assignment Pools Overview
- Address-Assignment Pool Configuration Overview
external-authority

Syntax

external-authority;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.

When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 891

Extended DHCP Local Server Overview | 718

Address-Assignment Pools Overview
failure-action

Syntax

```
failure-action (clear-binding | clear-binding-if-interface-up | log-only);
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit system services dhcp-relay dhcpv6 group group-name liveness-detection],
[edit system services dhcp-local-server group group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the action the router (or switch) takes when a liveness detection failure occurs.

Options

**Default:** clear-binding

- **clear-binding** — The DHCP client session is cleared when a liveness detection failure occurs, except when maintain-subscribers interface-delete setting is configured and active.

- **clear-binding-if-interface-up** — The DHCP client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up. Use this setting to distinguish failures from between a liveness detection failure due to a local network error, and a host disconnecting from the network. If the client binding is in the maintain-binding Finite State Machine (FSM) state when the liveness detection failure detection occurs, then the binding is not deleted. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

- **log-only** — A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure and maintain the client binding. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

Required Privilege Level

routing — To view this statement in the configuration.
routing-control — To add this statement to the configuration.
### RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Liveness Detection Overview</td>
<td>858</td>
</tr>
<tr>
<td>Configuring Detection of DHCP Local Server Client Connectivity with BFD</td>
<td>866</td>
</tr>
<tr>
<td>Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD</td>
<td>860</td>
</tr>
<tr>
<td>Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients</td>
<td>869</td>
</tr>
<tr>
<td>Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients</td>
<td>862</td>
</tr>
</tbody>
</table>
family (Security Forwarding Options)

Syntax

```plaintext
family {
    inet6 {
        mode (drop | flow-based | packet-based);
    }
    iso {
        mode packet-based;
    }
    mpls {
        mode packet-based;
    }
}
```

Hierarchy Level

```
[edit security forwarding-options]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Determine the protocol family to be used for packet forwarding.

**NOTE:** Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- MPLS Overview
falling-threshold (Health Monitor)

Syntax

falling-threshold percentage;

Hierarchy Level

[edit snmp health-monitor]

Release Information

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

Description

Set the lower threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored variable, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

- **percentage**—Lower threshold for the alarm entry.

Range: 1 through 100

Default: 70 percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

- rising-threshold | 2207

Configuring Health Monitoring
fast-start (LLDP-MED)

Syntax

```
fast-start count;
```

Hierarchy Level

```
[edit protocols lldp-med]
```

Release Information

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

Description

Configure the number of Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) advertisements sent from the switch in the first second after it has detected an LLDP-MED device (such as an IP telephone).

Options

```
count—Number of advertisements.
```

Range: 1 through 10

Default: 3

Required Privilege Level

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

RELATED DOCUMENTATION

- `show lldp` | 2680
- Configuring LLDP-MED (CLI Procedure) | 665
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
fields (for Interface Profiles)

Syntax

```plaintext
fields {
  field-name;
}
```

Hierarchy Level

```plaintext
[edit accounting-options interface-profile profile-name]
```

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

Description
Statistics to collect in an accounting-data log file for an interface.

Options
field-name—Name of the field:

- input-bytes—Input bytes
- input-errors—Generic input error packets
- input-multicast—Input packets arriving by multicast
- input-packets—Input packets
- input-unicast—Input unicast packets
- output-bytes—Output bytes
- output-errors—Generic output error packets
- output-multicast—Output packets sent by multicast
- output-packets—Output packets
- output-unicast—Output unicast packets

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

**Syntax**

```plaintext
file certificate-filename;
```

**Hierarchy Level**

```plaintext
[edit security certificates certification-authority ca-profile-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

**Options**

- `certificate-filename`—File from which to read the digital certificate.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

*Specifying a File to Read the Digital Certificate*
file (Associating with a Profile)

Syntax

```
file filename;
```

Hierarchy Level

```
[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]
```

Release Information

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

Description

Specify the accounting log file associated with the profile.

Options

`filename`—Name of the log file. You must specify a filename already configured in the file statement at the [edit accounting-options] hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Interface Profile
- Configuring the Filter Profile
- Configuring the MIB Profile
- Configuring the Routing Engine Profile
file (Configuring a Log File)

Syntax

```
file filename {
    archive-sites {
        site-name;
    }
    backup-on-failure (master-and-slave | master-only);
    compress;
    files number;
    nonpersistent;
    push-backup-to-master;
    size bytes;
    start-time time;
    transfer-interval minutes;
}
```

Hierarchy Level

[edit accounting-options]

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

Description
Specify a log file to be used for accounting data.

Options

`filename`—Name of the file in which to write accounting data.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

`Configuring Accounting-Data Log Files`
Configuring Flat-File Accounting for Layer 2 Wholesale

Configuring Flat-File Accounting for Extensible Subscriber Services Management

Flat-File Accounting Overview
file (System Logging)

Syntax

```
file filename {
    facility severity;
    archive {
        files number;
        size size;
        (no-world-readable | world-readable);
    }
    explicit-priority;
    match "regular-expression";
    match-strings string-name;
    structured-data {
        brief;
    }
}
```

Hierarchy Level

```
[edit system syslog]
```

Release Information

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

Description

Configure the logging of system messages to a file.

Options

- **facility**—Class of messages to log. To specify multiple classes, include multiple `facility severity` statements. For a list of the facilities, see Junos OS System Logging Facilities.

- **file filename**—File in the `/var/log` directory in which to log messages from the specified facility. To log messages to more than one file, include more than one `file` statement.

- **severity**—Severity of the messages that belong to the facility specified by the paired `facility` name. Messages with severities of the specified level and higher are logged. For a list of the severities, see System Log Message Severity Levels.

The remaining statements are explained separately. See CLI Explorer.
Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Directing System Log Messages to a Log File
file (System Logging)

Syntax

```plaintext
file name {
  allow-duplicates;
  archive name password password routing-instance routing-instance <(binary-data | no-binary-data)> <files files>
    <size bytes> <start-time start-time> <transfer-interval minutes> <(world-readable | no-world-readable)>;
  contents (any | authorization | change-log | conflict-log | daemon | dfe | external | firewall | ftp |
    interactive-commands | kernel | local0 | lpr | mail | news | ntp | pfe | privileged | security | syslog | user | uucp) { ... }
  explicit-priority;
  match match;
  match-strings [ match-strings ... ];
  structured-data (brief | detail);
}
```

Hierarchy Level

```plaintext
[edit system syslog]
```

Release Information

Statement introduced before Junos OS Release 12.1X47 for SRX Series.

Description

Specify the file in which to log data.

Options

- `filename`—Specify the name of the file in which to log data.
- `allow-duplicates`—Do not suppress the repeated messages.
- `any`—Specify all facilities information.
  - `alert`—Specify the conditions that should be corrected immediately.
  - `critical`—Specify the critical conditions.
  - `emergency`—Specify the conditions that cause security functions to stop.
  - `error`—Specify the general error conditions.
  - `info`—Specify the information about normal security operations.
  - `none`—Do not specify any messages.
  - `notice`—Specify the conditions that should be handled specifically.
- **warning**—Specify the general warning conditions.
- **archive**—Specify the archive file information.
  - **archive-sites**—Specify a list of destination URLs for the archived log files.
    - **url**—Specify the primary and failover URLs to receive archive files.
  - **binary-data**—Mark file such that it contains binary data.
  - **no-binary-data**—Do not mark the file such that it contains binary data.
  - **files**—Specify the number of files to be archived. Range: 1 through 1000 files.
  - **size**—Specify the size of files to be archived. Range: 65,536 through 1,073,741,824 bytes.
  - **world-readable**—Allow any user to read the log file.
  - **no-world-readable**—Do not allow any user to read the log file.
  - **start-time**—Specify the start time for file transmission. Enter the start time in the yyyy-mm-dd.hh:mm format.
  - **transfer-interval**—Specify the frequency at which to transfer the files to archive sites.
- **authorization**—Specify the authorization system.
- **change-log**—Specify the configuration change log.
- **conflict-log**—Specify the configuration conflict log.
- **daemon**—Specify the various system processes.
- **dfc**—Specify the dynamic flow capture.
- **explicit-priority**—Include the priority and facility in messages.
- **external**—Specify the local external applications.
- **firewall**—Specify the firewall filtering system.
- **ftp**—Specify the FTP process.
- **interactive-commands**—Specify the commands executed by the UI.
- **kernel**—Specify the kernel information.
- **match**—Specify the regular expression for lines to be logged.
- **ntp**—Specify the NTP process.
- **pfe**—Specify the Packet Forwarding Engine.
- **security**—Specify the security-related information.
• **structured-data**—Log the messages in structured log format.
  • **brief**—Omit English language text from the end of the logged message.

• **user**—Specify the user processes.
  • **info**—Specify the informational messages.

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

**files**

**Syntax**

```
files number;
```

**Hierarchy Level**

```[edit accounting-options file filename]```

**Release Information**

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

**Description**

Specify the maximum number of log files to be used for accounting data.

**Options**

**number**—The maximum number of files. When a log file (for example, `profilelog`) reaches its maximum size, it is renamed `profilelog.0`, then `profilelog.1`, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for `number` is 3 and the default value is 10.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

| Configuring Accounting-Data Log Files |
filter-duplicates

Syntax

filter-duplicates;

Hierarchy Level

[edit snmp]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Filter duplicate Get, GetNext, or GetBulk SNMP requests.

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

RELATED DOCUMENTATION

Filtering Duplicate SNMP Requests
Understanding the Implementation of SNMP on the QFabric System
Example: Configuring SNMP
filter-profile

Syntax

```
filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

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

Description
Create a profile to filter and collect packet and byte count statistics and write them to a file in the `/var/log` directory. To apply the profile to a firewall filter, you include the `accounting-profile` statement at the `[edit firewall filter filter-name]` hierarchy level. For more information about firewall filters, see Firewall Filters Overview.

Options
```
profile-name—Name of the filter profile.
```

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

- Firewall Filters Overview
- Configuring the Filter Profile
finger

Syntax

```syntax
finger {
    connection-limit limit;
    rate-limit limit;
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Allow finger requests from remote systems to the local router.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Configuring Finger Service for Remote Access to the Router | 294 |
fingerprint-hash

Syntax

```plaintext
fingerprint-hash (md5 | sha2-256);
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information


Description

Configure the hash algorithm used by the SSH server when it displays key fingerprints.

Options

- **md5**—Enable the SSH server to use the MD5 algorithm.
- **sha2-256**—Enable the SSH server to use the sha2-256 algorithm. The default is sha2-256.

**NOTE:** The FIPS image does not permit the use of MD5 fingerprints. On systems in FIPS mode, **sha2-256** is the only available option.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring SSH Service for Remote Access to the Router or Switch | 294
flow-tap-dtcp

Syntax

flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
  }
}

Hierarchy Level

[edit system services]

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Configure Dynamic Tasking Control Protocol (DTCP) sessions to run over SSH in support of the flow-tap, FlowTapLite, or radius-flow-tap services. Note that the flow-tap feature is not supported on outbound, or egress, traffic. Only inbound, or ingress, traffic is supported.

This statement is required for DTCP-initiated subscriber secure policy mirroring (radius-flow-tap service).

Options

  connection-limit limit—(Optional) Maximum number of connections allowed.

  Range:  1 through 250
  Default:  75

  rate-limit limit— (Optional) Maximum number of connection attempts allowed per minute.

  Range:  1 through 250
  Default:  150

Required Privilege Level

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

RELATED DOCUMENTATION

  Configuring a DTCP-over-SSH Connection to the Mediation Device
force-discover (DHCP Client)

Syntax

force-discover;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number dhcp-client]

Release Information

Statement introduced in Junos OS Release 15.1X49-D80.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-client at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

Description

Forces the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Optional DHCP Client Attributes | 935
Minimum DHCP Client Configuration | 934
format (System Login)

Syntax

format (md5 | sha1 | sha256 | sha512);

Syntax (Junos OS Evolved)

format (md5 | sha256 | sha512);

Hierarchy Level

[edit system login password]

Release Information
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option sha1 is not supported in Junos OS Evolved.

Description
Configure the authentication algorithm for plain-text passwords.

Default
For Junos OS, the default encryption format is md5. For Junos-FIPS software, the default encryption format is sha1.

Options
The hash algorithm that authenticates the password can be one of these algorithms:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest. The option sha1 is not supported in Junos OS Evolved.
- **sha256**—Produces a 256-bit digest.
- **sha512**—Produces a 512-bit digest.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
**forward-snooped-clients (DHCP Local Server)**

**Syntax**

```plaintext
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

**Release Information**

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure how the DHCP local server filters and handles DHCP snooped packets on the specified interfaces.

**Options**

- **all-interfaces**—Perform the action on all interfaces.
- **configured-interfaces**—Perform the action only on interfaces that are configured as part of an interface group.
- **non-configured-interfaces**—Perform the action only on interfaces that are not configured as part of a group.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- DHCP Snooping Support | 898
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server
forward-snooped-clients (DHCP Relay Agent)

Syntax

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

Hierarchy Level

```
[edit forwarding-options dhcpc-relay],
[edit forwarding-options dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcpc-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcpc-relay],
[edit routing-instances routing-instance-name forwarding-options dhcpc-relay]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure how DHCP relay agent filters and handles DHCP snooped packets on the specified interfaces. The router or switch determines the DHCP snooping action to perform based on a combination of the forward-snooped-clients configuration and the configuration of either the allow-snooped-clients statement or the no-allow-snooped-clients statement.

The router (or switch) also uses this statement to determine how to handle snooped BOOTREPLY packets received on non-configured interfaces.

Options

- all-interfaces—Perform the action on all interfaces.

Default: On EX Series switches, the action is performed on all interfaces by default.

- configured-interfaces—Perform the action only on interfaces that are configured as part of an interface group.

- non-configured-interfaces—Perform the action only on interfaces that are not part of a group.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>DHCP Snooping Support</th>
<th>898</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent</td>
<td>902</td>
</tr>
</tbody>
</table>
**forwarding-class (VoIP)**

**Syntax**

```
forwarding-class <assured-forwarding | best-effort | expedited-forwarding |network-control>;
```

**Hierarchy Level**

```
[edit ethernet-switching-options voip interface <all | interface-name | access-ports>]

[edit switch-options voip interface <all | interface-name | access-ports>]
```

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

**Description**
For EX Series switches, configure the forwarding class used to handle packets on the VoIP interface.

**NOTE:** The **forwarding-class** statement at the `[edit ethernet-switching-options voip interface interface-name]` hierarchy level is used only by LLDP-MED for advertising capabilities VoIP phones. It is not used to classify VoIP traffic.

**Default**
Disabled.

**Options**

*class*—Forwarding class:

- **assured-forwarding**— Assured forwarding (AF)—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with three drop probabilities: low, medium, and high.
- **best-effort**—Provides no service profile. For the best effort forwarding class, loss priority is typically not carried in a class-of-service (CoS) value, and random early detection (RED) drop profiles are more aggressive.
- **expedited-forwarding**—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- **network-control**—Provides a typically high priority because it supports protocol control.

**Required Privilege Level**

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

RELATED DOCUMENTATION

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication | 550
forwarding-options (Security)

Syntax

```plaintext
forwarding-options {
  family {
    inet6 {
      mode (drop | flow-based | packet-based);
    }
    iso {
      mode packet-based;
    }
    mpls {
      mode packet-based;
    }
  }
}
```

Hierarchy Level

[edit security]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Determine how the `inet6`, `iso`, and `mpls` protocol families manage security forwarding options.

NOTE:

- Packet-based processing is not supported on the following SRX Series devices: SRX5400, SRX5600, and SRX5800.
- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the `set security forwarding-options family mpls mode packet-based` statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

Options

The remaining statements are explained separately. See CLI Explorer.
Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

MPLS Overview

Understanding Packet-Based Processing

Understanding Traffic Processing on Security Devices
ftp

Syntax

```
ftp {
    authentication-order [authentication-methods];
    connection-limit limit;
    rate-limit limit;
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

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

Description

Allow FTP requests from remote systems to the local router or switch.

Options

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring FTP Service for Remote Access to the Router or Switch | 293
global (Gx-Plus)

Syntax

```plaintext
global {
    include-ipv6;
    max-outstanding-requests number;
}
```

Hierarchy Level

[edit access gx-plus]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure global attributes for the Gx-Plus application.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Gx-Plus
group (DHCP Local Server)

Syntax

```plaintext
group group-name 
  access-profile profile-name;
authentication 
  password password-string;
username-include 
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description (device-interface | logical-interface);
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
  }
}
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name>;
interface interface-name 
  access-profile profile-name;
  exclude;
  overrides 
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82>;
    client-negotiation-match incoming-interface;
    delay-advertise 
      based-on (option-15 | option-16 | option-18 | option-37) 
      equals 
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      } 
      not-equals 
        ascii ascii-string;
        hexadecimal hexadecimal-string;
```
} 
starts-with { 
  ascii ascii-string; 
  hexadecimal hexadecimal-string; 
}
} 
} 
delay-time seconds; 
} 
delay-offer { 
based-on (option-60 | option-77 | option-82) { 
equals { 
  ascii ascii-string; 
  hexadecimal hexadecimal-string; 
}
not-equals { 
  ascii ascii-string; 
  hexadecimal hexadecimal-string; 
}
starts-with { 
  ascii ascii-string; 
  hexadecimal hexadecimal-string; 
}
} 
delay-time seconds; 
} 
dual-stack dual-stack-group-name; 
interface-client-limit number; 
process-inform { 
  pool pool-name; 
}
} 
rapid-commit; 
} 
service-profile dynamic-profile-name; 
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>; 
trace; 
upto upto-interface-name; 
}
liveness-detection {
failure-action (clear-binding | clear-binding-if-interface-up | log-only);
method {
bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
    }
    detection-time {
        threshold milliseconds;
    }
    session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
}
layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval interval;
}
}
}
overrides {
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match <option60-and-option82>:
  client-negotiation-match incoming-interface;
  delay-advertise {
    based-on (option-15 | option-16 | option-18 | option-37) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  delay-offer {
    based-on (option-60 | option-77 | option-82) {
      equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      not-equals {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
      starts-with {
        ascii ascii-string;
        hexadecimal hexadecimal-string;
      }
    }
    delay-time seconds;
  }
  delegated-pool;
  delete-binding-on-renegotiation;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  process-inform {
Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options

**group-name**—Name of the group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Extended DHCP Local Server Overview  |  718
- Grouping Interfaces with Common DHCP Configurations  |  853
- Using External AAA Authentication Services with DHCP  |  833
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets  |  873
group (DHCP Relay Agent)

Syntax

```plaintext
group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name interface-name;
            logical-system-name;
            mac-address mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    interface interface-name {
        access-profile profile-name;
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                }
            }
        }
    }
}
```
multiplier number;
no-adaptation;
transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
}
detection-time {
    threshold milliseconds;
}
session-mode (automatic | multihop | singlehop);
holddown-interval milliseconds;
}
}
}
overrides {
    allow-no-end-option;
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
    layer2-liveness-detection {
      max-consecutive-retries number;
      transmit-interval interval;
    }
  }
}
}
overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82>;
    client-negotiation-match incoming-interface;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-agent-remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82;
    }
    remote-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
    server-id-override
}
remote-id-mismatch disconnect;
route-suppression;
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Specify the name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration. A group must contain at least one interface. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

**group-name**—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Extended DHCP Relay Agent Overview</th>
<th>792</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)</td>
<td>783</td>
</tr>
<tr>
<td>Configuring Group-Specific DHCP Relay Options</td>
<td>856</td>
</tr>
<tr>
<td>Grouping Interfaces with Common DHCP Configurations</td>
<td>853</td>
</tr>
<tr>
<td>Using External AAA Authentication Services with DHCP</td>
<td>833</td>
</tr>
<tr>
<td><strong>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>DHCP Liveness Detection Using ARP and Neighbor Discovery Packets</td>
<td>873</td>
</tr>
</tbody>
</table>
group (System Services DHCP)

Syntax

group group-name {
    authentication {
        password password;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name;
            interface-name;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile;
    }
    interface interface-name {
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        exclude;
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
        }
    }
}
process-inform {
    pool pool-name;
}
rapid-commit;
}
service-profile service-profile-name
trace;
upto interface-name;
}
liveness-detection {
    failure-action {
        clear-binding;
        clear-binding-if-interface-up;
        log-only;
    }
    method {
        bfd {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval interval;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
    }
}
overides {
    delegated-pool pool-name;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
    service-profile service-profile-name;
}

Hierarchy Level

[edit system services dhcp-local-server dhcpv6]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure a group of interfaces that have a common configuration.

The remaining statements are explained separately. See CLI Explorer.

Options
• group-name—Name of the group.

NOTE: SRX Series devices do not support DHCP client authentication.

The remaining statements are explained separately. See CLI Explorer.

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

DHCP Overview | 909

DHCP Server Configuration Overview | 916
guest-vlan

Syntax

guest-vlan (vlan-id | vlan-name);

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names ])]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Specify the VLAN to which an interface is moved when no 802.1X supplicants are connected on the interface. The VLAN specified must already exist on the switch.

Default
None

Options

vlan-id—VLAN tag identifier of the guest VLAN.

vlan-name—Name of the guest VLAN.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448

Understanding Guest VLANs for 802.1X on Switches | 407
gx-plus (Gx-Plus)

Syntax

gx-plus {
    global {
        include-ipv6;
        max-outstanding-requests number;
    }
    partition partition-name {
        diameter-instance instance-name;
        destination-host hostname;
        destination-realm realm;
    }
}

Hierarchy Level

[edit access]

Release Information
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

Configuring Gx-Plus
health-monitor

Syntax

```
health-monitor {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

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

Description

Configure health monitoring.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

snmp—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Configuring Health Monitoring
- Understanding Health Monitoring
**hold-multiplier**

**Syntax**

```
hold-multiplier number;
```

**Hierarchy Level**

```
[edit protocols lldp]
```

**Release Information**

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

**Description**

Specify the multiplier used in combination with the `advertisement-interval` value to determine the length of time LLDP information is held before it is discarded. The default value is 4 (or 120 seconds).

**Default**

Disabled.

**Options**

- `number`—A number used as a multiplier.

**Range**: 2 through 10

**Default**: 4 (or 120 seconds)

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- `show lldp` | 2680
- Configuring LLDP (CLI Procedure) | 654
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
- Understanding LLDP | 653
holldown-interval

Syntax

holldown-interval milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.

Options
milliseconds—Interval specifying how long a BFD session must remain up before a state change notification is sent.

Range: 0 through 255,000
Default: 0

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
host (SSH Known Hosts)

Syntax

```
host hostname {
  dsa-key dsa-key;
  ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
  ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
  ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
  ed25519-key ed25519-key
  rsa-key rsa-key;
  rsa1-key rsa1-key;
}
```

Hierarchy Level

```
[edit security ssh-known-hosts]
```

Release Information

Statement modified in Junos OS Release 8.5.

Description

Configure the type of base-64 encoded host key.

Options

- **hostname**—Name of the SSH known host.
- **dsa-key dsa-key**—Digital Signature Algorithm (DSA) for SSH version 2
- **ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key**—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key**—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key**—Elliptic Curve Digital Signature Algorithm (ECDSA)
- **ed25519-key ed25519-key**—Elliptic Curve Digital Signature Algorithm (ed25519 for ECDSA)
- **rsa-key rsa-key**—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2
- **rsa1-key rsa1-key**—RSA public key algorithm, which supports encryption and digital signatures for SSH version 1

Required Privilege Level

- **security**—To view this statement in the configuration.
- **security-control**—To add this statement to the configuration.
RELATED DOCUMENTATION

Generating SSL Certificates for Secure Web Access (SRX Series Devices) | 340
Generating a Self-Signed SSL Certificate Automatically | 342
**hostkey-algorithm**

**Syntax**

```
hostkey-algorithm {
  (no-ssh-dss | ssh-dss);
  (no-ssh-rsa | ssh-rsa);
  (no-ssh-ecdsa | ssh-ecdsa);
  (no-ssh-ed25519 | ssh-ed25519);
}
```

**Hierarchy Level**

```
[edit system services ssh]
```

**Release Information**
Statement introduced in Junos OS Release 11.2.

**Description**
Allow or disallow a host-key algorithm to authenticate another host through SSH protocol. The host-key uses RSA, ECDSA, ED25519, and DSS algorithms.

The following are the behaviors when the `hostkey-algorithm` option is configured with SSH client and SSH server:

- On SSH client the host-key algorithms that are supported when talking to a server are:
  - a. RSA: Equal or greater-than to 1024 bit
  - b. ECDSA: 256, 384, or 521 bit
  - c. ED25519: 256 bit
  - d. DSS: 1024 bit
- On SSH server the host-key algorithms that are generated and stored are:
  - a. RSA: 2048 bit
  - b. ECDSA: 256 bit
  - c. ED25519: 256 bit
  - d. DSS: 1024 bit

**Options**
• **ssh-ecdsa**—Allow generation of an ECDSA host-key. Key pair sizes of 256, 384, or 521 bits are compatible with ECDSA.

• **ssh-dss**—Allow generation of a 1024-bit DSA host-key.

  NOTE: DSA keys are not supported in FIPS, so the **ssh-dss** option is not available on systems operating in FIPS mode.

• **ssh-rsa**—Allow generation of RSA host-key. Key pair sizes greater than or equal to 1024 are compatible with RSA.

• **no-ssh-dss**—Do not allow generation of a 1024-bit Digital Signature Algorithm (DSA) host-key.

• **no-ssh-ecdsa**—Do not allow generation of an Elliptic Curve Digital Signature Algorithm (ECDSA) host-key.

• **no-ssh-rsa**—Do not allow generation of an RSA host-key.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Generating SSL Certificates for Secure Web Access (SRX Series Devices)</th>
<th>340</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generating a Self-Signed SSL Certificate Automatically</td>
<td>342</td>
</tr>
</tbody>
</table>
host-name (DHCP Relay Agent)

Syntax

host-name name;

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82]

Release Information
Command introduced in Junos OS Release 16.2.

Description
Supports the addition of vendor-specific hostname in the option 82, suboption 9 field of DHCPv4 control messages on server-facing interfaces. The hostname can be a string of characters such as Juniper-AB-1.

Junos OS automatically adds the remaining vendor-specific information as per RFC 4243, Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option. The Juniper Networks enterprise ID is 2636. The hostname is option-data 1 (the location is option-data 2). The DHCPv4 relay strips the suboption data from replies from the server before it relays the packets out the client facing interface.

This feature can be useful, in conjunction with operator-developed tools, for troubleshooting DHCP servers and providing service assurances. For example, a central DHCP server can log the information, and operators can query the hostname to track and troubleshoot subscriber IP information and network attachment points.

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

Syntax

```plaintext
http {
    interfaces [ interface-names ];
    port port;
}
```

Hierarchy Level

```
[edit system services web-management]
```

Release Information

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

Description

Configure the port and interfaces for HTTP service, which is unencrypted.

Options

`interfaces [ interface-names ]`—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

| Configuring Management Access for the EX Series Switch (J-Web Procedure) |
| J-Web Interface User Guide |

| https  | 1839 |
| port  | 2072 |
| web-management  | 2431 |
**https**

**Syntax**

```plaintext
https {
  interfaces [interface-names];
  local-certificate name;
  port port;
}
```

**Hierarchy Level**

[edit system services web-management]

**Release Information**

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

**Description**

Configure the secure version of HTTP (HTTPS) service, which is encrypted.

**Options**

**interfaces [interface-names]**—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

**local-certificate name**—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Configuring Management Access for the EX Series Switch (J-Web Procedure)*
- *J-Web Interface User Guide*
ignore-port-bounce

**Syntax**

```
ignore-port-bounce;
```

**Hierarchy Level**

```
[edit protocols dot1x authenticator interface interface-name mac-radius]
```

**Release Information**

Statement introduced in Junos OS Release 17.3R1 for EX Series switches.

**Description**

Ignore the port-bounce command contained in a Change of Authorization (CoA) request. CoA requests are RADIUS messages that are used to dynamically modify an authenticated user session already in progress. CoA requests are sent from the authentication, authorization, and accounting (AAA) server to the switch, and are typically used to change the VLAN for the host based on device profiling. End devices such as printers do not have a mechanism to detect the VLAN change, so they do not renew the lease for their DHCP address in the new VLAN. The port bounce feature is used to force the end device to initiate DHCP re-negotiation by causing a link flap on the authenticated port. There is no configuration required to enable the port bounce feature.

**Default**

The port bounce feature is supported by default. If you do not configure the `ignore-port-bounce` statement, the switch responds to a port-bounce command by flapping the link to re-initiate DHCP negotiation for the end device.

**Required Privilege Level**

routing

**RELATED DOCUMENTATION**

Understanding RADIUS-Initiated Changes to an Authorized User Session | 392
immediate-update

Syntax

immediate-update;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

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

Description

Configure the router or switch to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Per-Subscriber Session Accounting

RADIUS Servers and Parameters for Subscriber Access
include-ipv6 (Gx-Plus)

Syntax

include-ipv6;

Hierarchy Level

[edit access gx-plus global]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Include IPv6 subscribers in Gx-Plus provisioning requests.

Default

By default, IPv6 subscribers are not included.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Gx-Plus Global Attributes

Configuring Gx-Plus
include-irb-and-l2

Syntax

include-irb-and-l2;

Hierarchy Level

[edit forwarding-options dhcp dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp relay ... relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp relay ... relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]

Release Information


NOTE: The EX Series switches that support the include-irb-and-l2 statement are the EX4300, EX4600, and EX9200 switches.

Description

Include both the integrated routing and bridging (IRB) interface name and Layer 2 interface name in the circuit-id or remote-id value in the DHCP option 82 information. VLAN tags are global.

For leasequery and bulk leasequery operations that involve integrated routing and bridging (IRB) interfaces, you must configure DHCP relay agent to include the layer 2 interface name along with IRB name in the circuit ID of option 82. DHCP relay agent uses the layer 2 interface name when using leasequery or bulk leasequery to restore the lease database.

When you configure the include-irb-and-l2 statement without including the no-vlan-interface statement, the format is as follows:

• Bridge domain:
(fe | ge)-fpc/pic/port.subunit:bridge-domain-name+irb.subunit

- VLAN:

(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit

NOTE: For remote systems, the subunit is required and is used to differentiate an interface.

When you configure both the **include-irb-and-l2** statement and the **use-vlan-id** statement, the format is as follows:

(fe | ge)-fpc/pic/port.subunit:svlan-id-vlan-id+irb.subunit

NOTE: The svlan-id-vlan-id represents the VLANs associated with the bridge domain.

When you configure both the **include-irb-and-l2** and **no-vlan-interface-name** statements, the format is as follows:

(fe | ge)-fpc/pic/port.subunit+irb.subunit

When you configure both the **include-irb-and-l2** and **use-interface-description** statements, the format displays the description for the Layer 2 interface:

l2_descr:vlan-name+irb.subunit

If you configure both the **include-irb-and-l2** and **use-interface-description** statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name:

(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit

When you configure the **include-irb-and-l2** statement with both the **no-vlan-interface-name** and **use-interface-description** statements, the format displays as follows:

l2_descr+irb.subunit
If you configure the `include-irb-and-l2` statement with both the `no-vlan-interface-name` and `use-interface-description` statements, and no description is found for the Layer 2 interface, the format displays as follows:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

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

**RELATED DOCUMENTATION**

- *Including a Textual Description in DHCP Options*
- *Using DHCP Relay Agent Option 82 Information* | 739
- *Configuring DHCPv6 Relay Agent Options*
infranet-controller

Syntax

```bash
infranet-controller hostname {
    address ip-address;
    interface interface-name;
    password password;
    port port-number;
}
```

Hierarchy Level

```bash
[edit services unified-access-control]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the switch's connection to the Junos Pulse Access Control Service network access control (NAC) device.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
interface (802.1X)

Syntax

```plaintext
interface (all | [ interface-names ]) {
    disable;
    guest-vlan (vlan-name | vlan-id);
    lldp-med-bypass;
    mac-radius <restrict>;
    maximum-requests number;
    no-reauthentication;
    quiet-period seconds;
    reauthentication {
        interval seconds;
    }
    retries (802.1X) number;
    server-fail (deny | permit | use-cache | vlan-id | vlan-name);
    server-reject-vlan (vlan-id | vlan-name) {
        eapol-block;
        block-interval block-interval;
    }
    server-timeout seconds;
    supplicant (single | single-secure | multiple);
    supplicant-timeout seconds;
    transmit-period seconds;
}
```

Hierarchy Level

```
[edit protocols dot1x authenticator]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authentication for Port-Based Network Access Control for all interfaces or for specific interfaces.

Options

all—Configure all interfaces for 802.1X authentication.

[ interface-names ]— List of names of interfaces to configure for 802.1X authentication.
The remaining statements are explained separately.

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

**RELATED DOCUMENTATION**

| show dot1x | 2644 |
| Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440 |
| Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch | 448 |
| Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528 |
| Configuring MAC RADIUS Authentication on an EX Series Switch | 427 |
| Configuring 802.1X Interface Settings (CLI Procedure) | 390 |

*Configuring 802.1X Authentication (J-Web Procedure)*
interface (Access Control Service)

Syntax

interface interface-name;

Hierarchy Level

[edit services unified-access-control infranet-controller]

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Specify the interface through which the switch will connect to the Junos Pulse Access Control Service.

Options

interface-name—Name of the interface that will connect the switch to the Access Control Service.

Required Privilege Level

routing—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520 |
| Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523 |
interface (Captive Portal)

**Syntax**

```plaintext
interface (all | [interface-names]) {
    quiet-period seconds;
    retries number-of-retries;
    server-timeout seconds;
    session-expiry seconds;
    supplicant (multiple | single | single-secure);
}
```

**Hierarchy Level**

```plaintext
[edit services captive-portal]
```

**Release Information**

Statement introduced in Junos OS Release 10.1 for EX Series switches.

**Description**

Configure captive portal authentication for all interfaces or for specific interfaces.

**Options**

- `all`—All interfaces to be configured for captive portal authentication.
- `[interface-names]`—List of names of interfaces to be configured for captive portal authentication.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492
interface (DHCP Local Server)

Syntax

```plaintext
interface interface-name {
    access-profile profile-name;
    exclude;
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82 | incoming-interface>;
        client-negotiation-match incoming-interface;
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                delay-time seconds;
            }
            delay-offer {
                based-on (option-60 | option-77 | option-82) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
            }
        }
    }
}
```
delay-time seconds;
}
dual-stack dual-stack-group-name;
interface-client-limit number;
rapid-commit;
}
service-profile dynamic-profile-name;
short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
trace;
upto upto-interface-name;
}

Hierarchy Level

[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options upto and exclude introduced in Junos OS Release 9.1.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.

NOTE: DHCP values are supported in integrated routing and bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently supports only static DHCP configurations.
Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the overrides option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the upto-interface-name must be the same as the device name of the interface-name.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Extended DHCP Local Server Overview</th>
<th>718</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping Interfaces with Common DHCP Configurations</td>
<td>853</td>
</tr>
<tr>
<td>Using External AAA Authentication Services with DHCP</td>
<td>833</td>
</tr>
</tbody>
</table>
interface (DHCP Relay Agent)

Syntax

```plaintext
interface dhcp-interface-name {
    access-profile profile-name;
    exclude;
    overrides {
        allow-no-end-option
        allow-snooped-clients;
        always-write-giaddr;
        always-write-option-82;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82 | incoming-interface>;
        client-negotiation-match incoming-interface;
        disable-relay;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
        proxy-mode;
        relay-source
        replace-ip-source-with;
        send-release-on-delete;
        trust-option-82;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

```plaintext
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information
Statement introduced in Junos OS Release 8.3.
Options upto and exclude introduced in Junos OS Release 9.1.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP or DHCPv6 relay agent is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP local server. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

NOTE: DHCP values are supported in integrated routing and bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations.

Options
exclude—Exclude an interface or a range of interfaces from the group. This option and the overrides option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

overrides—Override the specified default configuration settings for the interface. The overrides statement is described separately.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the upto-interface-name must be the same as the device name of the interface-name.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
### RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>Grouping Interfaces with Common DHCP Configurations</td>
<td>853</td>
</tr>
<tr>
<td>Using External AAA Authentication Services with DHCP</td>
<td>833</td>
</tr>
</tbody>
</table>
interface (LLDP)

Syntax

interface (all | interface-name) {

disable;

power-negotiation {

disable;
}
}

Hierarchy Level

[edit protocols lldp]

Release Information

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

Description

Configure Link Layer Discovery Protocol (LLDP) on all interfaces or on a specific interface.

NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command `set protocols lldp interface me0` generates the following error message:

```
error: name: 'me0': Invalid interface
error: statement creation failed: interface
```

Issuing the command `set protocols lldp interface vme` generates the following error message:

```
error: name: 'vme': Invalid interface
error: statement creation failed: interface
```

Default

None

Options
all—All interfaces on the switch.

interface-name—Name of a specific interface.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Configuring LLDP (CLI Procedure)</th>
<th>654</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
<td>661</td>
</tr>
<tr>
<td>Understanding LLDP</td>
<td>653</td>
</tr>
</tbody>
</table>
**interface (LLDP-MED)**

**Syntax**

```plaintext
interface (all | interface-name) {
    disable;
    location {
        elin number;
        civic-based {
            what number;
            country-code code;
            ca-type {
                number {
                    ca-value value;
                }
            }
        }
    }
}
```

**Hierarchy Level**

```
[edit protocols lldp-med]
```

**Release Information**

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

**Description**

Configure Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) on all interfaces or on a specific interface.

**Default**

Not enabled

**Options**

- all—All interfaces on the switch.

  **interface-name**—Name of a specific interface.

  The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>RELATED DOCUMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>show lldp</td>
</tr>
<tr>
<td>Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</td>
</tr>
<tr>
<td>Configuring LLDP-MED (CLI Procedure)</td>
</tr>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
</tr>
</tbody>
</table>
interface (Static MAC Bypass)

Syntax

```
interface [interface-names];
```

Hierarchy Level

```
[edit protocols dot1x authenticator authentication-profile-name static mac-address],
[edit ethernet-switching-options authentication-whitelist mac-address],
[edit switch-options authentication-whitelist mac-address]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.

Options

- `interface-names`—List of interfaces.

Required Privilege Level

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

RELATED DOCUMENTATION

- show dot1x static-mac-address | 2658
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492
interface (System Services DHCP)

Syntax

```plaintext
interface interface-name {
    exclude;
    overrides {
        interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

[edit system services dhcp-local-server dhcpv6 group group-name]

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

Options

- **interface-name**—Name of the interface.
- **trace**—Enable tracing of the interface specified by the interface-name argument.
- **upto upto-interface-name**—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the upto-interface-name must be the same as the device name of the interface-name.

Required Privilege Level

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

RELATED DOCUMENTATION

- DHCP Overview | 909
interface (VoIP)

Syntax

```
interface (all | [interface-name] | access-ports) {
    vlan vlan-name ;
    forwarding-class <assured-forwarding | best-effort | expedited-forwarding | network-control> ;
}
```

Hierarchy Level

- For platforms with ELS:

  ```
  [edit switch-options voip]
  ```

- For platforms without ELS:

  ```
  [edit ethernet-switching-options voip],
  ```

Release Information

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

Description

Enable voice over IP (VoIP) on interfaces.

Options

- all—Enable VoIP on all interfaces.

- `interface-name`—Enable VoIP on a specific interface.

- all—(Switches without ELS only) Enable VoIP on all access ports.

The remaining statements are explained separately.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch</th>
<th>528</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication</td>
<td>550</td>
</tr>
<tr>
<td>Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support</td>
<td>544</td>
</tr>
</tbody>
</table>
# interface-client-limit (DHCP Local Server)

## Syntax

```
interface-client-limit number;
```

## Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
```

## Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

## Description
Set the maximum number of DHCP subscribers or DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Default
No limit

Options

number—Maximum number of clients allowed.

Range: 1 through 500,000

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

RELATED DOCUMENTATION

- Specifying the Maximum Number of DHCP Clients Per Interface | 837
- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
interface-client-limit (DHCP Relay Agent)

Syntax

interface-client-limit number;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group interface interface-name overrides]

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Set the maximum number of DHCP (or DHCPv6) subscribers or clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

Default
No limit

Options

number—Maximum number of clients allowed.

Range: 1 through 500,000

Required Privilege Level

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>dhcp-relay</th>
<th>1665</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>Configuring Group-Specific DHCP Relay Options</td>
<td>856</td>
</tr>
<tr>
<td>Overriding the Default DHCP Relay Configuration Settings</td>
<td>803</td>
</tr>
</tbody>
</table>
interface-delete (Subscriber Management or DHCP Client Management)

Syntax

interface-delete;

Hierarchy Level

[edit system services subscriber-management maintain-subscriber]

Release Information

Statement introduced in Junos OS Release 11.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.

On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.

Required Privilege Level

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

RELATED DOCUMENTATION

  Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events
interface-description-format

Syntax

interface-description-format {
  exclude-adapter;
  exclude-channel;
  exclude-sub-interface;
}

Hierarchy Level

[edit access profile profile-name radius options]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
exclude-adapter and exclude-sub-interface options added in Junos OS Release 10.4.
exclude-channel option added in Junos OS Release 17.3R1.

Description
Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attributes such as NAS-Port-ID (87) or Calling-Station-ID (31).

The default format for nonchannelized interfaces is as follows:

interface-type-slot/adapter/port.subinterface[:svlan-vlan]

For example, consider physical interface ge-1/2/0, with a subinterface of 100 and SVLAN identifier of 100. The interface description used in the NAS-Port-ID is ge-1/2/0.100:100. If you exclude the subinterface, the description becomes ge-1/2/0:100.

The default format for channelized interfaces is as follows:

interface-type-slot/adapter/channel.subinterface[:svlan-vlan]

The channel information (logical port number) is determined by this formula:

Logical port number = 100 + (actual-port-number x 20) + channel-number.

For example, consider a channelized interface 3 on port 2 where the:

- Physical interface is xe-0/1/2:3.
- Subinterface is 4.
- SVLAN is 5.
• VLAN is 6.

Using the formula, the logical port number = 100 + (2 x 20) + 3 = 143. Consequently, the default interface description is xe-0/1/143.4-5.6. If you exclude the channel information, the description becomes xe-0/1/2.4-5.6.

**Options**

**exclude-adapter** — (Optional) Exclude the adapter from the interface description.

**exclude-channel** — (Optional) Exclude the channel information from the interface description.

**exclude-sub-interface** — (Optional) Exclude the subinterface from the interface description.

**Required Privilege Level**

admin—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

*Interface Text Descriptions for Inclusion in RADIUS Attributes*

*RADIUS Servers and Parameters for Subscriber Access*
interface-name (DHCP Local Server)

Syntax

interface-name;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

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

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients | 834
interface-profile

Syntax

```
interface-profile profile-name {
    allow-clear;
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

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

Description
Create a profile to filter and collect error and packet statistics and write them to a file in the `/var/log` directory. You can specify an interface profile for either a physical or a logical interface.

Options

`profile-name`—Name of the interface profile.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

- Configuring the Interface Profile
- Accounting Options Configuration
interface-traceoptions (System Services DHCP)

Syntax

interface-traceoptions {
  file {
    filename ;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}

Hierarchy Level

[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the interface interface-name trace statement at the [edit system services group group-name] hierarchy level to enable the tracing operation on the specific interfaces.

Options
file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named jdhcpd in the directory /var/log. If you include the file statement, you must specify a filename.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1000
Default: 3 files
flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- **all**—Trace all events
- **dhcpv6-packet**—Trace DHCPv6 packet decoding operations.
- **dhcpv6-packet-option**—Trace DHCPv6 option decoding operations.
- **dhcpv6-state**—Trace changes in state for DHCPv6 operations.
- **packet**—Trace packet decoding operations
- **packet-option**—Trace DHCP option decoding operations
- **state**—Trace changes in state

**match regular-expression**—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** \( xk \) to specify KB, \( xm \) to specify MB, or \( xg \) to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

| DHCP Overview | 909 |
| DHCP Server Configuration Overview | 916 |
interfaces (ARP)

Syntax

interfaces {
    interface-name {
        aging-timer minutes;
    }
}

Hierarchy Level

[edit system arp]

Release Information
Statement introduced before Junos OS Release 9.4.

Description
Specify the Address Resolution Protocol (ARP) aging timer in minutes for a logical interface.

Options
aging-timer minutes—Time between ARP updates, in minutes.

Range: 1 through 240

Default: 20

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

RELATED DOCUMENTATION

| DHCP Overview | 909 |
| DHCP Server Configuration Overview | 916 |
interfaces (Security Zones)

Syntax

```plaintext
interfaces interface-name {
    host-inbound-traffic {
        protocols protocol-name {
            except;
        }
        system-services service-name {
            except;
        }
    }
}
```

Hierarchy Level

[edit security zones functional-zone management],
[edit security zones security-zone zone-name]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the set of interfaces that are part of the zone.

Options

`interface-name` — Name of the interface.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Security Zones
interval (Accounting Options)

Syntax

interval minutes;

Hierarchy Level

[edit accounting-options class-usage-profile profile-name],
[edit accounting-options filter-profile profile-name],
[edit accounting-options interface-profile profile-name],
[edit accounting-options mib-profile profile-name],
[edit accounting-options routing-engine-profile profile-name]

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

Description
Specify how often statistics are collected for the accounting profile.

Options

minutes—Length of time between each collection of statistics.

Range: 1 through 2880 minutes
Default: 30 minutes

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

RELATED DOCUMENTATION

Configuring the Interface Profile
Configuring the Filter Profile
Configuring the MIB Profile
Configuring the Routing Engine Profile
interval (Access Control Service)

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit services unified-access-control]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the time between continuity check messages for the switch's connection with the Junos Pulse Access Control Service. The specified value must be less than the value specified for `timeout`.

Options

- `seconds`—Time between continuity check messages, in seconds.

Range: 1 through 9999 seconds

Default: 30 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
interval (Health Monitor)

Syntax

interval seconds;

Hierarchy Level

[edit snmp health-monitor],
[edit snmp health-monitor idp]

Release Information
Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.3 for the [edit snmp health-monitor idp] hierarchy level.

Description
Interval between samples.

Options
seconds—Time between samples, in seconds.

Range: 1 through 2147483647 seconds

Default: 300 seconds

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

RELATED DOCUMENTATION

Configuring the Interval
interval (Health Monitor)

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit snmp health-monitor]
```

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure the interval between sampling of the object being monitored by the health monitor.

Options
- `seconds`—Time between samples, in seconds.

Range: 1 through 2147483647 seconds
Default: 300 seconds

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

RELATED DOCUMENTATION

- Configuring Health Monitoring
ip-address-first

Syntax

ip-address-first;

Hierarchy Level

[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

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

RELATED DOCUMENTATION

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use  | 891

Extended DHCP Local Server Overview  | 718

Address-Assignment Pools Overview
keep-incoming-circuit-id (DHCP Relay Agent)

Syntax

```plaintext
keep-incoming-circuit-id ;
```

Hierarchy Level

- [edit forwarding-options dhcp-relay relay-option-82 circuit-id],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 circuit-id],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id]

Release Information

Description
Specify that the `jdhcpd` process keeps the incoming circuit ID and prepends the ID with the locally generated ID (in the format, `generated-id + incoming-id`) before sending the leasequery packet to the DHCP server.

This configuration is required for leasequery and bulk leasequery operations when subscriber authentication is based on the circuit ID, and enables leasequery and bulk leasequery to restore the agent circuit identifier/agent remote identifier (ACI/ARI) pair and to use the circuit ID to authenticate subscribers.

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

RELATED DOCUMENTATION

| Using DHCP Relay Agent Option 82 Information | 739 |
keep-incoming-remote-id (DHCP Relay Agent)

Syntax

```
keep-incoming-remote-id ;
```

Hierarchy Level

- [edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
- [edit forwarding-options dhcp-relay relay-option-82 circuit-id],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 XXXcircuit-id],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],

Release Information


Description

Specify that the `jdhcpd` process keeps the incoming remote ID and prepends the ID with the locally generated ID (in the format, `generated-id + incoming-id`) before sending the leasequery packet to the DHCPv6 server.

This configuration is required for leasequery and bulk leasequery operations when subscriber authentication is based on the remote ID, and enables leasequery and bulk leasequery to restore the agent circuit identifier/agent remote identifier (ACI/ARI) pair and to use the remote ID to authenticate subscribers.

Use the statement at the `[edit ... dhcpv6]` hierarchy level to configure DHCPv6 support.

Required Privilege Level

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

RELATED DOCUMENTATION

- Using DHCP Relay Agent Option 82 Information | 739
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets | 830
key (Authentication Keychain)

Syntax

```plaintext
key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    key-name authentication-key-name;
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
}
```

Hierarchy Level

```
[edit security authentication-key-chains key-chain key-chain-name]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.4.

Description

Configure the authentication element.

Options

- **key**—Each key within a keychain is identified by a unique integer value.

Range: 0 through 63

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION
Example: Configuring BFD Authentication for Securing Static Routes

Example: Configuring Hitless Authentication Key Rollover for IS-IS
key-chain (Security)

Syntax

```plaintext
key-chain key-chain-name {
    description text-string;
    key key {
        algorithm (md5 | hmac-sha-1);
        options (basic | isis-enhanced);
        key-name authentication-key-name;
        secret secret-data;
        start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
}
```

Hierarchy Level

[edit security authentication-key-chains]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 17.4.

Description

Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options

**key-chain-name**—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.
RELATED DOCUMENTATION

authentication-key-chains | 1516

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols | 286

Example: Configuring BFD Authentication for Securing Static Routes

Example: Configuring Hitless Authentication Key Rollover for IS-IS
key-exchange

Syntax

key-exchange [algorithm1 algorithm2...];

Hierarchy Level

[edit system services ssh]

Release Information

Description
Specify the set of Diffie-Hellman key exchange methods that the SSH server can use.

Options
One or more of the following Diffie-Hellman key exchange methods:

- **curve25519-sha256**—The EC Diffie-Hellman key exchange method on Curve25519 with SHA2-256.
- **dh-group1-sha1**—The Diffie-Hellman group1 algorithm using SHA-1.
- **dh-group14-sha1**—The Diffie-Hellman group14 algorithm using SHA-1.
- **ecdh-sha2-nistp256**—The ECDH key exchange method with ephemeral keys generated on the nistp256 curve.
- **ecdh-sha2-nistp384**—The ECDH key exchange method with ephemeral keys generated on the nistp384 curve.
- **ecdh-sha2-nistp521**—The ECDH key exchange method with ephemeral keys generated on the nistp521 curve.
- **group-exchange-sha1**—The group exchange algorithm using SHA-1.
- **group-exchange-sha2**—The group exchange algorithm using SHA-2.

**NOTE:** The key-exchange represents a set. To configure key-exchange:

user@host#set system services ssh key-exchange [ecdh-sha2-nistp256 group-exchange-sha1]
NOTE: Table 61 on page 1891 shows the supportability of Diffie-Hellman key exchange methods on FIPS mode.

<table>
<thead>
<tr>
<th>Diffie-Hellman key exchange methods</th>
<th>Supported on FIPS mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>curve25519-sha256</td>
<td>No</td>
</tr>
<tr>
<td>dh-group1-sha1</td>
<td>No</td>
</tr>
<tr>
<td>dh-group14-sha1</td>
<td>Yes</td>
</tr>
<tr>
<td>ecdh-sha2-nistp256</td>
<td>Yes</td>
</tr>
<tr>
<td>ecdh-sha2-nistp384</td>
<td>Yes</td>
</tr>
<tr>
<td>ecdh-sha2-nistp521</td>
<td>Yes</td>
</tr>
<tr>
<td>group-exchange-sha1</td>
<td>No</td>
</tr>
<tr>
<td>group-exchange-sha2</td>
<td>No</td>
</tr>
</tbody>
</table>

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

**RELATED DOCUMENTATION**

- Configuring SSH Service for Remote Access to the Router or Switch | 294
- ciphers | 1564
- macs | 1933
layer2-liveness-detection (Send)

Syntax

layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval seconds;
}

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection method],
[edit forwarding-options dhcp-relay group group-name liveness-detection method],
[edit forwarding-options dhcp-relay liveness-detection method],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method],
[edit system services dhcp-local-server dhcpv6 liveness-detection method],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection method],
[edit system services dhcp-local-server group group-name liveness-detection method],
[edit system services dhcp-local-server liveness-detection method],

Release Information
Statement introduced in Junos OS Release 17.4R1.

Description
Configure a router acting as a broadband network gateway (BNG) to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions.

The BNG sends ARP or ND request packets to each DHCP client at a configurable interval, then waits for a response. If it receives a response from a client before the interval times out, it sends another request to the client when the timer expires.

If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt.

If it receives a response from a client before the 30-second interval times out, it sends another request to the client when the timer expires. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This is the second retry attempt. If the BNG does not receive a response within this interval it resets the timer to 10 seconds and sends another request. The BNG continues to send requests at 10-second intervals until it either receives a response from the client before the interval times out or exhausts the number of retry attempts.
The first retry attempt uses a 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number of retries minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

If the BNG attempts all the retries and never receives a response from a client within the interval, the client session is declared to be down.

**NOTE:** The only option to the `failure-action` statement supported by Layer 2 liveness detection is `clear-binding`.

**Options**

- **max-consecutive-retries number**—Maximum number of consecutive times that the router sends an ARP request packet in the absence of an ARP response packet.
  - **Range:** 3 through 6 retries
  - **Default:** 3 retries

- **transmit-interval seconds**—Initial interval that the router waits for an ARP response after sending an ARP request packet to the client or waits for an ND response packet after sending an NG request packet to the client.
  - **Range:** 300 through 1800 seconds
  - **Default:** 300 seconds

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- [DHCP Liveness Detection Using ARP and Neighbor Discovery Packets](#) | 873
- [DHCP Liveness Detection Overview](#) | 858
layer2-unicast-replies

Syntax

layer2-unicast-replies;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

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

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview | 792
dhcp-relay | 1665
Idap-url

Syntax

```<ldap-url url-name>;
```

Hierarchy Level

```
[edit security certificates certification-authority ca-profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,

Description


Options

url-name—Name of the LDAP URL.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Specifying an LDAP URL
lease-time

Syntax

```
lease-time (length | infinite);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Request a specific lease time for the IP address. The lease time is the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server.

Default
If no lease time is requested by client, then the server sends the lease time. The default lease time on a Junos OS DHCP server is one day.

Options

- `seconds` — Request a lease time of a specific duration.

Range: 60 through 2147483647 seconds

- `infinite` — Request that the lease never expire.

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

RELATED DOCUMENTATION

- Configuring a DHCP Client (CLI Procedure) | 762
- interfaces
- unit
- family
lease-time (dhcp-client)

Syntax

```plaintext
lease-time seconds;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

Description

Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options

- `seconds`—Request time to negotiate and exchange information.

Required Privilege Level

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

RELATED DOCUMENTATION

- DHCP Overview | 909
liveness-detection

Syntax

liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit forwarding-options dhcp-relay group group-name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server group group-name]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure bidirectional failure detection timers and authentication criteria for static routes.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>DHCP Liveness Detection Overview</th>
<th>858</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Detection of DHCP Local Server Client Connectivity with BFD</td>
<td>866</td>
</tr>
<tr>
<td>Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD</td>
<td>860</td>
</tr>
<tr>
<td>Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients</td>
<td>869</td>
</tr>
<tr>
<td>Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients</td>
<td>862</td>
</tr>
<tr>
<td>DHCP Liveness Detection Using ARP and Neighbor Discovery Packets</td>
<td>873</td>
</tr>
</tbody>
</table>
**lldp**

**Syntax**

```plaintext
lldp {
  advertisement-interval seconds;  
  disable;
  hold-multiplier number;
  interface (all | interface-name) {  
    disable;
  }
  lldp-configuration-notification-interval seconds;
  management-address ip-management-address;
  mau-type
  port-description-type {  
    interface-alias;
    interface-description;
  }
  port-id-subtype {  
    interface-name;
    locally-assigned;
  }
  ptopo-configuration-maximum-hold-time seconds;
  ptopo-configuration-trap-interval seconds;
  traceoptions {  
    file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>:  
    flag flag <disable>;
  }
  transmit-delay (LLDP) seconds;
}
```

**Hierarchy Level**

```
[edit protocols],
[edit routing-instances routing-instance-name protocols]
```

**Release Information**


**Description**

Specify LLDP configuration parameters.

**Options**
The remaining statements are explained separately. See CLI Explorer.

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

**RELATED DOCUMENTATION**

- *Configuring LLDP*
lldp

Syntax

lldp {
    advertisement-interval seconds;
    disable;
    hold-multiplier number;
    interface (all | [interface-name]) {
        disable;
        power-negotiation {
            disable;
        }
    }
}  
lldp-configuration-notification-interval seconds;
management-address ip-management-address;
mau-type
netbios-snooping;
no-tagging;
ptopo-configuration-maximum-hold-time seconds;
ptopo-configuration-trap-interval seconds;
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <no-stamp> <replace>;
    flag flag <disable>;
}
transmit-delay seconds;
vlan-name-tlv-option (name | vlan-id);
}

Hierarchy Level

[edit protocols]

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

Description
Configure Link Layer Discovery Protocol (LLDP). The switch uses LLDP to advertise its identity and capabilities on a LAN, as well as to receive information about other network devices. LLDP is defined in the IEEE standard 802.1AB-2005.
The remaining statements are explained separately. See CLI Explorer.

NOTE: The transmit-delay and netbios-snooping options are not available on QFabric systems.

NOTE: On EX4300 switches, LLDP cannot be configured on the me0 or vme interface. Issuing the command set protocols lldp interface me0 generates the following error message:

```
error: name: 'me0': Invalid interface
error: statement creation failed: interface
```

Issuing the command set protocols lldp interface vme generates the following error message:

```
error: name: 'vme': Invalid interface
error: statement creation failed: interface
```

Default
LLDP is enabled.

The following statements have default values:

- **advertisement-interval**—The default value is 30 seconds. The allowable range is from 5 through 32768 seconds.
- **hold-multiplier**—The default value is 4. The allowable range is from 2 through 10.
- **ptopo-configuration-maximum-hold-time**—The default value is 300 seconds. The allowable range is from 1 through 2147483647 seconds.
- **transmit-delay**—The default value is 2 seconds. The allowable range is from 1 through 8192 seconds.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>RELATED DOCUMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>**show lldp</td>
</tr>
<tr>
<td>Configuring LLDP (CLI Procedure)</td>
</tr>
<tr>
<td>Understanding LLDP</td>
</tr>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
</tr>
</tbody>
</table>
**lldp-configuration-notification-interval**

**Syntax**

```
lldp-configuration-notification-interval seconds;
```

**Hierarchy Level**

```
[edit protocols lldp]
[edit routing-instances routing-instance-name protocols lldp]
```

**Release Information**
Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Specify how often SNMP trap notifications are generated as a result of LLDP database changes.

**Default**
SNMP trap notifications of LLDP database changes are disabled.

**Options**
- `seconds`—Time for the period of SNMP trap notifications about the LLDP database. This feature is disabled by default.

**Range:** 5 through 3600

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

**RELATED DOCUMENTATION**

- Configuring LLDP
- show lldp | 2680
lldp-med (Ethernet Switching)

Syntax

```
lldp-med {
    disable;
    fast-start number;
    interface (all | interface-name) {
        disable;
        location {
            elin number;
            civic-based {
                what number;
                country-code code;
                ca-type {
                    number {
                        ca-value value;
                    }
                }
            }
        }
    }
}
```

Hierarchy Level

[edit protocols]

Release Information

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

Description

Configure Link Layer Discovery Protocol–Media Endpoint Discovery. LLDP-MED is an extension of LLDP. The switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations for emergency services. LLDP-MED is defined in the standard ANSI/TIA-1057 by the Telecommunications Industry Association (TIA).

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

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

RELATED DOCUMENTATION

- show lldp | 2680
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Configuring LLDP-MED (CLI Procedure) | 665
lldp-med-bypass

Syntax

```
lldp-med-bypass;
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | interface-name )]
```

Release Information

Statement introduced in Junos OS Release 12.3 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Bypass the 802.1X authentication procedure for connecting multiple LLDP-MED end devices. Automatically add the learned MAC addresses of the end devices to the switch’s static MAC bypass list, and allow the devices to access the network. You can enable `lldp-med-bypass` only when the interface is also configured for 802.1X authentication of `multiple` supplicants.

Default

Disabled

Required Privilege Level

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>supplicant</th>
<th>2301</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Authentication on Switches</td>
<td>361</td>
</tr>
</tbody>
</table>
lldp-priority

Syntax

```
lldp-priority;
```

Hierarchy Level

```
[edit poe],
[edit poe fpc (all | slot-number)]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the switch to assign interfaces the power priority provided by the powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority configured on the switch interface.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring PoE on EX Series Switches (CLI Procedure)
lldp-tx-fast-init

Syntax

```lldp-tx-fast-init seconds;```

Hierarchy Level

```
[edit protocols lldp],
```

Release Information

Statement introduced in Junos OS Release 15.1R5 for EX Series switches.

Description

Configure the interval between transmissions to be made during a fast transmission period. A device that is enabled with Link Layer Discovery Protocol (LLDP) transmits LLDP packets to neighboring nodes at a specified time interval. Fast transmission periods are initiated when a new neighbor is detected, and cause LLDP packets to be transmitted at a shorter time interval than during normal operation of the protocol. The fast transmission period ensures that more than one LLDP packet is transmitted when a new neighbor is detected. The first transmission is immediate, and the subsequent transmissions occur at the specified fast transmission (TX) interval.

Options

- **seconds**—Specify the number of seconds between transmissions that occur during the fast transmission period.

Range: 1 through 8 seconds

Default: 1 second

Required Privilege Level

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

**RELATED DOCUMENTATION**

| show lldp | 2680 |
| Configuring LLDP (CLI Procedure) | 654 |
| Understanding LLDP and LLDP-MED on EX Series Switches | 661 |
| Understanding LLDPP | 653 |
local

Syntax

```
local certificate-name {
  certificate-key-string;
  load-key-file URL filename;
}
```

Hierarchy Level

```
[edit security certificates]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

Options

certificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file URL filename—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router’s or switch’s local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

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

RELATED DOCUMENTATION

Importing SSL Certificates for Junos XML Protocol Support
local-certificate

Syntax

```
local-certificate name;
```

Hierarchy Level

```
[edit system services service-deployment],
[edit system services web-management https],
[edit system services xnm-ssl],
[edit system services extension-service request-response thrift]
```

Release Information

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

Description

Import or reference an SSL certificate.

Specify the name of the local certificate to use. There is no default for local-certificate. The value for local-certificate should be the same as the name provided during the import of the certificate using the CLI configuration statement local at the [edit security certificates] hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
- Importing SSL Certificates for Junos XML Protocol Support
- local | 1911
local-server-group (DHCP Relay Agent Option)

Syntax

local-server-group local-server-group;

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay group-group-name relay-option (default-action | equals | starts-with)],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...
],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Forward DHCP client packets to the specified group of DHCP local servers when you use the DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces.

The local-server-group option is not supported for DHCPv6 relay agent.

Options

local-server-group—Name of DHCP local server group.

Required Privilege Level

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

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic
location (DHCP Relay Agent)

Syntax

```
location name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-82 vendor-specific],
[edit forwarding-options dhcp-relaygroup group-name relay-option-82 vendor-specific]
```

Release Information
Command introduced in Junos OS Release 16.2.

Description
Supports the addition of a vendor-specific location in the option 82, suboption 9 field of DHCPv4 control messages on server-facing interfaces. The location should be specified as interface, vlan ID, and if applicable, svlan ID. For example, `<ifd-name>::<vlan>` (ae0:100) or `<ifd-name>::<svlan>-<vlan>` (ae0:100-10).

Junos OS automatically adds the remaining vendor-specific information as per RFC 4243, *Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option*. The Juniper Networks enterprise ID is 2636. The the location is option-data 2 (the hostname is option-data 1). The DHCPv4 relay strips the suboption data from replies from the server before it relays the packets out the client facing interface.

This feature can be useful, in conjunction with operator-developed tools, for troubleshooting DHCP servers and providing service assurances. For example, a central DHCP server can log the information, and operators can query the hostname to track and troubleshoot subscriber IP information and network attachment points.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
location (LLDP-MED)

Syntax

```plaintext
location {
  elin number;
  civic-based {
    what number;
    country-code code;
    ca-type {
      number {
        ca-value value;
      }
    }
  }
}
```

Hierarchy Level

```
[edit protocols lldp-med interface (all | interface-name)]
```

Release Information

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

Description

For Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED), configure the location information. Location information is advertised from the switch to the MED. This information is used during emergency calls to identify the location of the MED.

The remaining statements are explained separately. See CLI Explorer.

Default

Disabled.

Required Privilege Level

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

RELATED DOCUMENTATION
location (SNMP)

Syntax

```
location location;
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the value of the MIB II `sysLocation` object, which is the physical location of the managed system.

Options

- `location`—Location of the local system. You must enclose the name within quotation marks (" ").

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the System Location for a Device Running Junos OS
location (System)

Syntax

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

Hierarchy Level

```
[edit system]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Configure the physical location of the device.

Options

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

• *postal-code postal-code*—Zip code or Postal code.

• *rack number*—Rack number.

• *vcoord vertical-coordinate*—Bellcore Vertical Coordinate.

**Required Privilege Level**

system—To view this statement in the configuration.

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

Syntax

lockout-period minutes;

Hierarchy Level

[edit system login retry-options]

Release Information
Statement introduced in Junos OS Release 11.2.

Description
Configure the amount of time before the user can attempt to log in to the router after being locked out due to the number of failed login attempts specified in the tries-before-disconnect statement.

Options
minutes—Amount of time before the user can attempt to log in after being locked out.

Default: Off

Range: 1 through 43200

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

RELATED DOCUMENTATION

Limiting the Number of User Login Attempts for SSH and Telnet Sessions
Login Retry Options  |  81
Example: Configuring Login Retry Options  |  84
retry-options  |  2205
clear system login lockout  |  2489
show system login lockout  |  2862
log

Syntax

```plaintext
log {
    session {
        client;
        all;
        dhcpv6 {
            client;
            server;
            relay;
            dynamic-server;
            all;
        }
    }
    server;
    relay;
}
```

Hierarchy Level

```
[edit system processes dhcp-service]
```

Release Information

Statement introduced in Junos OS Release 19.1R1 for SRX Series devices.

Description

Enable DHCP session log on the device. Session logs include the information on the session creation, deletion and renew events. You can use the session logs for monitoring and troubleshooting purposes.

Options

- `session`—Logs of the DHCP sessions.
- `client`—Log sessions of the DHCP client.
- `all`—Log sessions of the DHCP client, server and relay.
- `dhcpv6`—Log sessions of the DHCPv6.
- `client`—Log sessions of the DHCPv6 client.
- `dynamic-server`—Log sessions of the DHCPv6 dynamic server.
- `all`—Log sessions of the DHCPv6 client, server, relay and dynamic server.
- `server`—Log sessions of the DHCP server.
- relay—Log sessions of the DHCP relay.

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

### log-key-changes

**Syntax**

```
log-key-changes log-key-changes;
```

**Hierarchy Level**

```
[edit system services ssh]
```

**Release Information**

Statement introduced in Junos OS Release 17.4R1.

**Description**

Enable the `log-key-changes` to log the authorized SSH keys. When the `log-key-changes` configuration statement is enabled and committed, Junos OS logs the changes to the set of authorized SSH keys for each user (including the keys that were added or removed). Junos OS logs the differences since the last time the `log-key-changes` configuration statement was enabled. If the `log-key-changes` configuration statement was never enabled, then Junos OS logs all the authorized SSH keys.

**Required Privilege Level**
admin
logical-system-name (DHCP Local Server)

Syntax

```
logical-system-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...]
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level

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

RELATED DOCUMENTATION

- Using External AAA Authentication Services with DHCP | 833
login

Syntax

```plaintext
login {
    announcement text;

    class class-name {
        allow-hidden-commands;
        no-hidden-commands {
            except ['"regular expression or command 1" "regular expression or command 2" ...'];
        }
        access-end hh:mm;
        access-start hh:mm;
        ( allow-commands "(regular-expression1)|(regular-expression2)...") allow-commands-regexps ["regular expression1" "regular expression 2 " ... ];
        ( allow-configuration "(regular-expression1)|(regular-expression2)...") allow-configuration-regexps ["regular expression1" "regular expression 2 " ... ];
        allow-sources [ allow-sources ... ];
        allow-times [ allow-times ... ];
        allowed-days [ days of the week ];
        cli {
            prompt prompt;
        }
        configuration-breadcrumbs;
        confirm-commands ["regular expression or command 1" "regular expression or command 2" ... ] {
            confirmation-message;
        }
        ( deny-commands "(regular-expression1)|(regular-expression2)...") deny-commands-regexps ["regular expression1" "regular expression 2 " ... ];
        ( deny-configuration "(regular-expression1)|(regular-expression2)...") deny-configuration-regexps ["regular expression1" "regular expression 2 " ... ];
        deny-sources [ deny-sources ... ];
        deny-times [ deny-times ... ];
        idle-timeout minutes;
        logical-system logical-system-name;
        login-alarms;
        login-script login-script;
        login-tip;
        no-scp-server;
        no-sftp-server;
        permissions [ permissions ];
        satellite all;
        security-role (audit-administrator | crypto-administrator | ids-administrator | security-administrator);
        tenant tenant-system-name;
    }
}
```
message text;
password {
  change-type {set-transitions | character-set};
  format {md5 | sha1 | des};
  maximum-length length;
  minimum-changes number;
  minimum-length length;
}
retry-options {
  backoff-threshold number;
  backoff-factor seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}
user username {
  authentication {
    encrypted-password encrypted-password;
    no-public-keys;
    ssh-ecdsa name {
      from from;
    }
    ssh-ed25519 name {
      from from;
    }
    ssh-rsa name {
      from from;
    }
  }
  cli {
    prompt prompt;
  }
  class class-name;
  full-name full-name;
  uid uid-value;
}
}

Hierarchy Level
[edit system]
**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Configure user access to the device.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**
- Defining Junos OS Login Classes | 73
mac-address (DHCP Local Server)

Syntax

mac-address;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

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

RELATED DOCUMENTATION

Using External AAA Authentication Services with DHCP | 833
mac-address (DHCP Relay Agent)

Syntax

mac-address;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

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

RELATED DOCUMENTATION
mac-radius

Syntax

mac-radius <flap-on-disconnect> <restrict>;

Hierarchy Level

[edit protocols dot1x authenticator interface interface-name]

Release Information
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Option flap-on-disconnect introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Configure MAC RADIUS authentication for specific interfaces. MAC RADIUS authentication allows LAN access to permitted MAC addresses. When a new MAC address appears on an interface, the switch consults the RADIUS server to check whether the MAC address is a permitted address. If the MAC address is configured on the RADIUS server, the device is allowed access to the LAN.

If MAC RADIUS is configured, the switch first tries to get a response from the host for 802.1X authentication. If the host is unresponsive, the switch attempts to authenticate using MAC RADIUS.

To restrict authentication to MAC RADIUS only, use the restrict option. In restrictive mode, all 802.1X packets are eliminated and the attached device on the interface is considered a nonresponsive host.

Options

flap-on-disconnect—(Optional) When the RADIUS server sends a disconnect message to a supplicant, the switch resets the interface on which the supplicant is authenticated. If the interface is configured for multiple supplicant mode, the switch resets all the supplicants on the specified interface. This option takes effect only when the restrict option is also set.

restrict—(Optional) Restricts authentication to MAC RADIUS only. When mac-radius restrict is configured the switch drops all 802.1X packets. This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface, and eliminates the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
### RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Document</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x</td>
<td>2644</td>
</tr>
<tr>
<td>Example: Configuring MAC RADIUS Authentication on an EX Series Switch</td>
<td>427</td>
</tr>
<tr>
<td>Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch</td>
<td>440</td>
</tr>
<tr>
<td>Configuring MAC RADIUS Authentication (CLI Procedure)</td>
<td>426</td>
</tr>
<tr>
<td>Configuring 802.1X Interface Settings (CLI Procedure)</td>
<td>390</td>
</tr>
<tr>
<td>Understanding Authentication on Switches</td>
<td>361</td>
</tr>
</tbody>
</table>
macs

Syntax

```plaintext
macs [algorithm1 algorithm2...]
```

Hierarchy Level

```plaintext
[edit system services ssh]
```

Release Information

Statement introduced in Junos OS Release 11.2.
SHA-2 options introduced in Junos OS Release 12.1.

Description

Specify the set of message authentication code (MAC) algorithms that the SSH server can use to authenticate messages.

Options

Specify one or more of the following MAC algorithms to authenticate messages:

- **hmac-md5**—Hash-based MAC using Message-Digest 5 (MD5)
- **hmac-md5-96**—96-bits of hash-based MAC using MD5
- **hmac-md5-96-etm@openssh.com**—96-bits of hash-based Encrypt-then-MAC using MD5
- **hmac-md5-etm@openssh.com**—Hash-based Encrypt-then-MAC using MMD5
- **hmac-ripemd160**—Hash-based MAC using RIPEMD
- **hmac-ripemd160-etm@openssh.com**—Hash-based Encrypt-then-MAC using RIPEMD
- **hmac-sha1**—Hash-based MAC using secure hash algorithm-1 (SHA-1)
- **hmac-sha1-96**—96-bits of hash-based MAC using SHA-1
- **hmac-sha1-96-etm@openssh.com**—96-bits of hash-based Encrypt-then-MAC using SHA-1
- **hmac-sha1-etm@openssh.com**—Hash-based Encrypt-then-MAC using SHA-1
- **hmac-sha2-256**—256-bits of hash-based MAC using secure hash algorithm-2 (SHA-2)
- **hmac-sha2-256-etm@openssh.com**—Hash-based Encrypt-then-Mac using SHA-2
- **hmac-sha2-512**—512-bits of hash-based MAC using SHA-2
- **hmac-sha2-512-etm@openssh.com**—Hash-based Encrypt-then-Mac using SHA-2
- **umac-128-etm@openssh.com**—Encrypt-then-MAC using UMAC-128 algorithm specified in RFC4418
• umac-128@openssh.com—UMAC-128 algorithm specified in RFC4418
• umac-64-etm@openssh.com—Encrypt-then-MAC using UMAC-64 algorithm specified in RFC4418
• umac-64@openssh.com—UMAC-64 algorithm specified in RFC4418

NOTE: The macs configuration statement represents a set. Therefore, it must be configured as shown in the following example.

```
user@host#set system services ssh macs [hmac-md5 hmac-sha1]
```

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>key-exchange</th>
<th>1890</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciphers</td>
<td>1564</td>
</tr>
</tbody>
</table>
management-address

Syntax

management-address ip-management-address;

Hierarchy Level

[edit protocols lldp]

Release Information
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.

Default
The LLDP Management Address TLV uses the IP address of the switch's management Ethernet interface (me0), or the IP address of the virtual management Ethernet (VME) interface if the switch is a Virtual Chassis member.

Options
ip-management-address—You can specify either an IPv4 or an IPv6 management address for the switch.

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

RELATED DOCUMENTATION

| show lldp | 2680 |
| Understanding LLDP and LLDP-MED on EX Series Switches | 661 |
| Interfaces Overview for Switches |
| Understanding LLDP | 653 |
master-password

Syntax

```plaintext
master-password {
    plain-text-password
    iteration-count iteration-count;
    pseudorandom-function (hmac-sha1 | hmac-sha2-256 | hmac-sha2-512);
}
```

Hierarchy Level

```plaintext
[edit system]
```

Release Information
Statement introduced in Junos OS Release 16.2.

Description
Master password for $8$-based password-encryption. The master password is used as input to the password based key derivation function (PBKDF2) to generate an encryption key. The key is used as input to the Advanced Encryption Standard in Galois/Counter Mode (AES256-GCM). The plain text that the user enters is processed by the encryption algorithm (with key) to produce the encrypted text (cipher text).

Options
plain-text-password—Set the master password with plain text. The password quality is evaluated for strength, and the device gives feedback if weak passwords are used.

iteration-count—The number of iterations to use for the PBKDF2 hash function. The iteration count slows the hashing count, thus slowing attacker guesses.

    Default: 100
    Range: 10-10000

pseudorandom-function—Choose the algorithm to use for unpredictable number generation

    Values:
    - hmac-sha1—Hash-based MAC using secure hash algorithm-1 (SHA-1)
    - hmac-sha2-256—256-bits of hash-based MAC using SHA-2
    - hmac-sha2-512—512-bits of hash-based MAC using SHA-2

Required Privilege Level
admin
RELATED DOCUMENTATION

Hardening Shared Secrets in Junos OS | 200
request system decrypt password | 2522
mau-type

Syntax

```
mau-type;
```

Hierarchy Level

```
[edit protocols lldp]
```

Release Information

Statement introduced in Junos OS Release 15.1 for EX Series switches.

Description

Configure the switch to advertise information about the medium attachment unit (MAU) type. The MAU is a transceiver that interconnects the attachment unit interface (AUI) port on an attached host computer to an Ethernet cable. MAU types are defined in the IEEE 802.3 standard.

The MAU type is included in the MAC/PHY Configuration Status type, length, and value (TLV) message. TLVs are used by LLDP-capable devices to transmit information to neighbor devices. The MAC/PHY Configuration Status TLV is an organizationally defined TLV that advertises information about the physical interface. In addition to the MAU type, the MAC/PHY Configuration Status TLV also includes information such as autonegotiation status, support and advertised capabilities.

The MAU type cannot be changed by configuration; however, you must configure the `mau-type` statement to include the MAU type value in the MAC/PHY Configuration Status TLV.

Default

If the `mau-type` statement is not configured, the MAU type field of the MAC/PHY Configuration Status TLV contains the value `Unknown`.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding LLDP and LLDP-MED on EX Series Switches | 661
- Configuring LLDP
max-outstanding-requests (Diameter Applications)

Syntax

max-outstanding-requests number;

Hierarchy Level

[edit access gx-plus global],
[edit access ocs partition partition-name],
[edit access pcrf partition partition-name]

Release Information
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for OCS and PCRF partitions introduced in Junos OS Release 16.2 for MX Series routers.

Description
Limit the number of outstanding requests that the Diameter-based application (function) can retry to a remote server when the requests are improperly answered. Too many requests risks overloading the server and increases the chance of losing messages.

The gx-plus statement limits retries from the Gx-Plus function to the Gx-Plus server using the Gx and JSRC protocols. The ocs statement limits retries from the OCS function to the OCS server using the Gy protocol. The pcrf statement limits retries from the PCRF function to the PCRF server using the Gx protocol.

Options

number—Number of outstanding requests from the function to the server that can exist at any time.

Default: 40
Range: 2 through 40

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

RELATED DOCUMENTATION

Configuring Gx-Plus Global Attributes
Configuring Gx-Plus
Configuring the OCS Partition
max-pre-authentication-packets

Syntax

max-pre-authentication-packets value;

Hierarchy Level

[edit system services ssh]

Release Information
Statement introduced in Junos OS Release 12.3X48-D10.

Description
Define the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication.

Options

value—Maximum number of pre-authentication SSH packets that the server will accept.

Range: 20 through 2147483647.

Default: 128

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

RELATED DOCUMENTATION

The ssh Command | 299
max-sessions-per-connection

Syntax

```
max-sessions-per-connection number
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information
Statement introduced in Release 11.4 of Junos OS.

Description
Specify the maximum number of ssh sessions allowed per single SSH connection.

Options
Default: 10

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

RELATED DOCUMENTATION

- Configuring SSH Service for Remote Access to the Router or Switch | 294
- ssh | 2284
- Junos OS Security Configuration Guide
maximum-certificates

Syntax

```plaintext
maximum-certificates number;
```

Hierarchy Level

```plaintext
[edit security certificates]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.

Options

- `number`—Maximum number of peer digital certificates to be cached.

Range: 64 through 4,294,967,295 peer certificates

Default: 1024 peer certificates

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Maximum Number of Peer Certificates
maximum-hop-count

Syntax

maximum-hop-count number;

Hierarchy Level

[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (interface-name | interface-group)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description
Set the maximum allowed number of hops. This value is compared against the hops field in the BOOTP request message. BOOTP request messages that have a number in the hops field that exceeds maximum-hop-count are not forwarded. If you omit the maximum-hop-count statement, the default value is four hops.

Options

number—Maximum number of hops for BOOTP request messages.

Range: 1 through 16
Default: 4

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

RELATED DOCUMENTATION

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents
maximum-lease-time (DHCP)

Syntax

maximum-lease-time seconds;

Hierarchy Level

[edit system services dhcp],

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

Description
For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.

An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options
seconds—The maximum number of seconds the lease can be held.

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

**Syntax**

```
maximum-length length;
```

**Hierarchy Level**

```
[edit system login password]
```

**Release Information**

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

**Description**

Specify the maximum number of characters allowed in plain-text passwords. Newly created passwords must meet this requirement.

**Default**

For Junos-FIPS software, the maximum number of characters for plain-text passwords is 20. For Junos OS, no maximum is set.

**Options**

- `length`—The maximum number of characters the password can include.

**Range:** 1 to 64 characters

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
- password (Login) | 2060
maximum-lifetime

**Syntax**

```
maximum-lifetime days;
```

**Hierarchy Level**

```
[edit system login passwords]
```

**Release Information**

Statement introduced in Junos OS Release 18.4R1 for ACX Series, EX Series, QFX Series, MX Series, PTX Series.

**Description**

Specify the maximum password lifetime in days. A user who has the required permissions is able to control the maximum lifetime of a password. If the age of the password reaches the maximum lifetime configured, the password expires and has to be changed. If your password has expired, you cannot commit the configuration until the password is changed. Password expiry is applicable only for local user accounts.

**NOTE:** You cannot configure the same password every time the password expires. Older passwords cannot be configured on password expiry. Therefore, **maximum-lifetime** can be committed only after configuring **minimum-reuse**, else commit fails and error is displayed on commit.

If **maximum-lifetime** is configured, password expiry validation check is performed at the time of login and at the time of commit based on the password timestamp. For passwords configured before **minimum-reuse** configuration is committed, the timestamp of the passwords is the time at which any configuration under system login hierarchy is committed following the commit for **minimum-reuse**. For passwords configured after **minimum-reuse** configuration is committed, the timestamp of the passwords is the time at which those passwords are committed.

**Options**

- **days**—The maximum duration of a password where the password expires after the maximum duration is reached.

**Range:** 30-365

**Required Privilege Level**

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

**Syntax**

```plaintext
maximum-requests number;
```

**Hierarchy Level**

```plaintext
[edit protocols dot1x authenticator interface (all | [interface-names])]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

**Description**

For 802.1X authentication, configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out.

**Default**

Two retransmission attempts

**Options**

- `number`—Number of retransmission attempts.

**Range:** 1 through 10

**Default:** 2

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring 802.1X Authentication (J-Web Procedure)
maximum-time

Syntax

maximum-time seconds;

Hierarchy Level

[edit system login retry-options]

Release Information

Description
Configure the maximum time available for the user to enter the username and password for logging on to a router before the connection is closed.

Options
seconds—Maximum length of time that the connection remains open for the user to enter a username and password to log in. If the user remains idle and does not enter a username and password within the configured maximum-time, the connection is closed.

Range: 20 through 300
Default: 120

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Limiting the Number of User Login Attempts for SSH and Telnet Sessions</th>
<th>82</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry-options</td>
<td>2205</td>
</tr>
</tbody>
</table>
**message**

**Syntax**

message text;

**Hierarchy Level**

[edit system login]

**Release Information**

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

**Description**

Configure a system login message. This message appears before a user logs in.

You can format the message using the following special characters:

- \n— New line
- \t— Horizontal tab
- ’— Single quotation mark
- “— Double quotation mark
- \— Backslash

**Options**

text— Text of the message.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

*Configuring Junos OS to Display a System Login Message*

announcement | 1501
method

Syntax

```junos
method {
  bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    detection-time {
      threshold milliseconds;
    }
    session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
  }
  layer2-liveness-detection {
    max-consecutive-retries number;
    transmit-interval interval;
  }
}
```

Hierarchy Level

```junos
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection],
[edit system services dhcp-local-server group group-name liveness-detection],
[edit system services dhcp-local-server liveness-detection]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description
Configure the liveness detection method.

NOTE: The bfd stanza is not available at the [edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection method] or [edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection hierarchy levels].

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

| DHCP Liveness Detection Overview | 858 |
| Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869 |
| Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862 |
| DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 873 |
mib-profile

Syntax

```plaintext
mib-profile profile-name {
  file filename;
  interval minutes;
  object-names {
    mib-object-name;
  }
  operation operation-name;
}
```

Hierarchy Level

[edit accounting-options]

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Create a MIB profile to collect selected MIB statistics and write them to a file in the `/var/log` directory.

NOTE: Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

Options

- `profile-name`—Name of the MIB statistics profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the MIB Profile
minimum-changes

Syntax

minimum-changes number;

Hierarchy Level

[edit system login passwords]

Release Information

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

Description

Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.

This statement is used in combination with the change-type statement. If the change-type is character-sets, then the number of character sets included in the password is checked against the specified minimum. If change-type is set-transitions, then the number of character set changes in the password is checked against the specified minimum.

Default

For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3.

Options

number—The minimum number of character sets (or character set changes) required for the password.

Required Privilege Level

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

RELATED DOCUMENTATION

| change-type | 1562 |
minimum-character-changes

Syntax

minimum-character-changes number;

Hierarchy Level

[edit system login passwords]

Release Information
Statement introduced in Junos OS Release 18.3R1.

Description
Specify the minimum number of character changes between old and new passwords. Newly created passwords must meet this requirement. A user who has the required permissions is able to configure the number of character changes between passwords. If the number of character changes between the old password and new password is greater than or equal to the configured value for minimum number of character changes, new password is accepted and if it is less, new password is rejected.

Options
number—The minimum number of character changes between old and new passwords.

Range: 4 to 15 characters

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

RELATED DOCUMENTATION

Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
password (Login) | 2060
minimum-interval

Syntax

minimum-interval milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd transmit-interval]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the transmit-interval minimal-interval and minimum-receive-interval statements.

Options
milliseconds — Specify the minimum interval value for BFD liveliness detection.

Range: 1 through 255,000

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
minimum-length

Syntax

minimum-length length;

Hierarchy Level

[edit system login passwords]

Release Information

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

Description

Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-upper-cases, minimum-punctuations, minimum-lower-cases, and so on.

Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.

Default

For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10.

Options

length—The minimum number of characters the password must include.

Range: 6 to 20 characters

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

maximum-length | 1945
minimum-lifetime

Syntax

minimum-lifetime days;

Hierarchy Level

[edit system login passwords]

Release Information
Statement introduced in Junos OS Release 18.4R1 for ACX Series, EX Series, QFX Series, MX Series, PTX Series.

Description
Specify the minimum password lifetime in days. A user who has the required permissions is able to control the minimum lifetime of a password. You cannot change the password if the age of the password does not exceed the minimum lifetime value configured. When you change a password, the age of the existing password is retrieved based on the time at which the password was configured and the current time is fetched. If the age of the password is less than or equal to the configured value for minimum-lifetime, the new password is not accepted and error message is displayed. If the age of the password is more than the configured value for minimum-lifetime, the new password is accepted.

NOTE: minimum-lifetime can be committed only after configuring minimum-reuse as minimum lifetime works in coordination with password history requirements, else commit fails and error is displayed on commit.

If minimum-lifetime is configured, password change for a user is accepted or rejected based on the timestamp of the current password for that user. For passwords configured before minimum-reuse configuration is committed, the timestamp of the passwords is the time at which any configuration under system login hierarchy is committed following the commit for minimum-reuse. For passwords configured after minimum-reuse configuration is committed, the timestamp of the passwords is the time at which those passwords are committed.

Options

days—The minimum duration of a password. You cannot change the password until the minimum duration is reached.
Range: 1-30 days

Required Privilege Level
system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197

password (Login) | 2060
minimum-lower-cases

Syntax

minimum-lower-cases number;

Hierarchy Level

[edit system login password]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Specify the minimum number of lower-case letters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as minimum-length, minimum-punctuations, minimum-upper-cases, and so on.

Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.

Options
number—The minimum number of lower-case letters required for the password.

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

RELATED DOCUMENTATION
Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
password (Login) | 2060
**minimum-numerics**

**Syntax**

```
minimum-numerics number;
```

**Hierarchy Level**

```
[edit system login password]
```

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Specify the minimum number of numeric class characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as `minimum-length`, `minimum-punctuations`, `minimum-lower-cases`, and so on.

Using several password minimum requirement options will cause the `minimum-length` to be reset if the total sum of the required minimums exceeds the `minimum-length` setting.

**Options**

`number`—The minimum number of numeric class characters required for the password.

**Required Privilege Level**

system—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
- password (Login) | 2060
**minimum-punctuations**

**Syntax**

```
minimum-punctuations number;
```

**Hierarchy Level**

```
[edit system login password]
```

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Specify the minimum number of punctuation class characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as `minimum-length`, `minimum-upper-cases`, `minimum-lower-cases`, and so on.

Using several password minimum requirement options will cause the `minimum-length` to be reset if the total sum of the required minimums exceeds the `minimum-length` setting.

**Options**

- `number`—The minimum number of punctuation class characters required for the password.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
- password (Login) | 2060
minimum-receive-interval

Syntax

minimum-receive-interval milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the minimum interval at which the local routing device (or switch) must receive a reply from a neighbor with which it has established a BFD session.

Options
milliseconds — Specify the minimum receive interval value.

Range: 1 through 255,000

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
# minimum-reuse

## Syntax

```
minimum-reuse number;
```

## Hierarchy Level

```
[edit system login passwords]
```

## Release Information

Statement introduced in Junos OS Release 18.3R1.

## Description

Specify the the number of old passwords which should not match the new password. Newly created passwords must meet this requirement. A user who has the required permissions is able to control the number of old passwords that need to be compared. The number of old passwords to compare with the new password depends on the value configured. If a match is found between the new password and any of the old passwords, Junos OS device rejects the new password and aborts. If the new password is different from the configured number of old passwords, new password is accepted.

## Options

- **number**—The minimum number of old passwords which should not match the new password.

## Range

1 to 20 passwords

## Required Privilege Level

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

## RELATED DOCUMENTATION

- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
- password (Login) | 2060
minimum-time

Syntax

minimum-time seconds;

Hierarchy Level

[edit system login retry-options]

Release Information

Statement introduced in Junos OS Release 8.0.

Description

Configure the minimum time available for the user to enter a password to log on to a router before the connection is closed.

Options

seconds—Minimum length of time that the connection remains open while the user is attempting to enter a password to log in.

Range: 20 through 60

Default: 20

Required Privilege Level

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

RELATED DOCUMENTATION

Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82
retry-options | 2205
minimum-upper-cases

**Syntax**

```
minimum-upper-cases number;
```

**Hierarchy Level**

```
[edit system login password]
```

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Specify the minimum number of upper-case letters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as `minimum-length`, `minimum-punctuations`, `minimum-lower-cases`, and so on.

Using several password minimum requirement options will cause the `minimum-length` to be reset if the total sum of the required minimums exceeds the `minimum-length` setting.

**Options**

- **number**—The minimum number of upper-case letters required for the password.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Changing the Requirements for Junos OS Plain-Text Passwords | 197
- password (Login) | 2060
minimum-wait-time

Syntax

minimum-wait-time seconds;

Hierarchy Level

[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (interface-name | interface-group)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description
To set the minimum allowed number of seconds in the secs field of the BOOTP message, include the minimum-wait-time statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the secs field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

The default value for the minimum wait time is zero (0) seconds. If the minimum wait time is 0 and the secs field in the BOOTP request message is 0, the device forwards the packet.

Options
seconds—Minimum wait time the BOOTP client has waited before packets are forwarded.
Range: 0 to 30,000
Default: 0

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

RELATED DOCUMENTATION

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents
multi-domain

Syntax

multi-domain {
  max-data-session max-data-sessions;
  packet-action (drop-and-log | shutdown);
  recovery-timeout seconds;
}

Hierarchy Level

[edit protocols dot1x authenticator interface interface-name]

Release Information
Statement introduced in Junos OS Release 18.3R1.

Description
Configure multi-domain authentication to restrict the number of authenticated data and VoIP sessions on the port. Multi-domain authentication is an extension of multiple supplicant mode for 802.1X authentication, and is designed to support VoIP and data clients on the same interface. The interface is divided into two domains; one is the data domain and the other is the voice domain.

In multiple supplicant mode, any number of VoIP or data sessions can be authenticated; the number of sessions can be restricted using MAC limiting, but there is no way to apply the limit specifically to either data or VoIP sessions. Multi-domain authentication maintains separate session counts based on the domain type.

The data device can be authenticated using 802.1X authentication or MAC RADIUS authentication. Multi-domain authentication does not enforce the order of authentication. For best results, the VoIP device should be authenticated before the data device.

You can configure the maximum number of authenticated data sessions allowed on the interface using the max-data-session statement. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed.

If a new client attempts to authenticate on the interface after the maximum session count has been reached, the default action is to drop the packet and generate an error log message. You can also configure the action to shut down the interface. The port can be manually recovered from the down state by issuing the clear dot1x recovery-timeout command, or can recover automatically after a recovery timeout period. To configure automatic recovery, use the recovery-timeout option.

Options
**max-data-session** **max-data-sessions**—The number of authenticated data sessions are allowed in the data domain on the 802.1X interface.

**Range:** 1 through 1,000 sessions

**Default:** 1

**packet-action (drop-and-log | shutdown)**—Define the action the switch should take on packets that exceed the limit of authenticated sessions allowed on the interface. The number of data sessions is configured using the **max-data-session** option. The number of VoIP sessions is not configurable; only one authenticated VoIP session is allowed.

- **drop-and-log**—Drop the packet and generate an error syslog message.
- **shutdown**—Shut down the interface.

**Default:** The default packet action is to drop the packet and generate an error syslog message.

**recovery-timeout seconds**—If you configure the packet action with the shutdown option and you enable the recovery timeout, the interface is temporarily disabled when the maximum number of authenticated sessions is reached. The interface will recover automatically after the number of seconds specified.

**Range:** 60 through 3600 seconds

**Default:** none

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>authenticator</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
</tr>
<tr>
<td>interface (IEEE 802.1x)</td>
</tr>
</tbody>
</table>
**multicast-client**

**Syntax**

```
multicast-client <address>;
```

**Hierarchy Level**

```
[edit system ntp]
```

**Release Information**

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

For Network Time Protocol (NTP), configure the local router or switch to listen for multicast messages on the local network to discover other servers on the same subnet.

**Options**

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

**Default:** 224.0.1.1.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Understanding NTP Time Servers*
- *Configuring NTP Authentication Keys*
- *Configuring the Switch to Listen for Multicast Messages Using NTP*
multicast-client

Syntax

```
multicast-client <address>;
```

Hierarchy Level

```
[edit system ntp]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For NTP, configure the SRX Series device to listen for multicast messages on the local network to discover other servers on the same subnet.

Options

`address`—(Optional) One or more IP addresses. If you specify addresses, the SRX Series device joins those multicast groups.

Default: 224.0.1.1.

Required Privilege Level

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

RELATED DOCUMENTATION

ntp | 2005
multiplier

Syntax

multiplier number;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the number of hello packets not received by the neighbor before Bidirectional Forwarding Detection (BFD) declares the neighbor down.

Options

number—Maximum allowable number of hello packets missed by the neighbor.

Range: 1 through 255
Default: 3

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
name-server (Access)

Syntax

```
name-server address
```

Hierarchy Level

```
[edit access address-assignment pool <name> family (inet | inet6) dhcp-attributes]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Specify the DNS server IP address for an address-assignment pool.

Required Privilege Level

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

RELATED DOCUMENTATION

| address-assignment (Access) | 1475 |
name-server (System Services)

Syntax

```yaml
name-server {
    address {
        routing-instance routing-instance;
    }
}
```

Hierarchy Level

```
[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
`routing-instance` options introduced in Junos OS Release 19.2R1 under the `[edit system]` hierarchy level only.

Description

Configure one or more Domain Name System (DNS) name servers.

Options

**address**—Address of the name server. To configure multiple name servers, include a maximum of three `address` options.

**routing-instance routing-instance**—Configure name of the routing instance through which the name server is reachable.

NOTE: The only routing instance supported is mgmt_junos.

Required Privilege Level

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

RELATED DOCUMENTATION

_Configuring a DNS Name Server for Resolving Hostnames into Addresses_

**nas-ip-address**

**Syntax**

```plaintext
nas-ip-address ip-address;
```

**Hierarchy Level**

```
[edit system radius-options attributes]
```

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Configure the NAS-IP address for outgoing RADIUS packets.

**Options**

- **ip-address**—IP address of the network access server (NAS) that requests user authentication.

**Required Privilege Level**

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
- Configuring RADIUS Authentication (QFX Series or OCX Series) | 244
**nas-port-extended-format**

**Syntax**

```plaintext
nas-port-extended-format {
    adapter-width bits;
    ae-width bits;
    atm {
        adapter-width bits;
        port-width bits;
        slot-width bits;
        vci-width bits;
        vpi-width bits;
    }
    port-width bits;
    pw-width bits;
    slot-width bits;
    stacked-vlan-width bits;
    vlan-width bits;
}
```

**Hierarchy Level**

```plaintext
[edit access profile profile-name radius options]
```

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
**ae-width** option added in Junos OS Release 12.1.
**atm** option added in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
**atm** option supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
**pw-width** option added in Junos OS Release 15.1.

**Description**

Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width in bits of the fields in the NAS-Port attribute.

The NAS-Port attribute specifies the physical port number of the NAS that is authenticating the user, and is formed by a combination of the physical port’s slot number, port number, adapter number, VLAN ID, and S-VLAN ID. The NAS-Port extended format specifies the number of bits (bit width) for each field in the NAS-Port attribute: slot, adapter, port, aggregated, Ethernet, VLAN, and S-VLAN.
NOTE: The combined total of the widths of all fields for a subscriber must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.

Options

adapter-width width—Number of bits in the adapter field.

ae-width width—(Ethernet subscribers only) Number of bits in the aggregated Ethernet identifier field.

atm—Specify width for fields for ATM subscribers.

port-width width—Number of bits in the port field.

pw-width width—(Ethernet subscribers only) Number of bits in the pseudowire field. Appears in the Cisco NAS-Port-Info AVP (100).

slot-width width—Number of bits in the slot field.

stacked-vlan-width width—Number of bits in the SVLAN ID field.

cvi-width width—(ATM subscribers only) Number of bits in the ATM virtual circuit identifier (VCI) field.

vlan-width width—Number of bits in the VLAN ID field.

vpi-width width—(ATM subscribers only) Number of bits in the ATM virtual path identifier (VPI) field.

NOTE: The total of the widths must not exceed 32 bits, or the configuration will fail.

Required Privilege Level

admin—to view this statement in the configuration.

admin-control—to add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Access Profile Options for Interactions with RADIUS Servers

RADIUS Servers and Parameters for Subscriber Access
nas-port-id-format (Subscriber Management)

Syntax

```plaintext
nas-port-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    interface-text-description;
    nas-identifier;
    order (agent-circuit-id | agent-remote-id | interface-description | interface-text-description | nas-identifier |
        postpend-vlan-tags);
    postpend-vlan-tags;
}
```

Hierarchy Level

```
[edit access profile profile-name radius options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Options `interface-text-description`, `order`, and `postpend-vlan-tags` introduced in Junos OS Release 15.1.

Description

Specify the optional information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

When you specify the values for the NAS-Port-ID, you can configure the values to appear in either the default order or a custom order of your choice.

NOTE: The default and custom order methods are mutually exclusive. The configuration fails if you attempt to configure a NAS-Port-ID that includes values in both types of orders.

To specify that the optional values appear in the default order in the NAS-Port-ID, configure the values directly under the `nas-port-id-format` statement. The default order is as follows, in which the `#` character is the delimiter:

```plaintext
nas-identifier # interface-description # interface-text-description # agent-circuit-id # agent-remote-id # postpend-vlan-tags
```
To specify a custom order for the NAS-Port-ID string, you use the order option. Include the order option before each optional value you want to include in the string, in the order in which you want the options to appear. For example, the configuration, order interface-text-description order nas-identifier order agent-remote-id produces the following NAS-Port-ID, in which the # character is the delimiter:

interface-text-description # nas-identifier # agent-remote-id

**Default**
The router includes the interface description in the NAS-Port-ID when no optional values are specified.

**Options**
- **agent-circuit-id**—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.
- **agent-remote-id**—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.
- **interface-description**—Include the interface description (interface identifier).
- **interface-text-description**—Include the textual interface description (the text description that is statically configured in the CLI).
- **nas-identifier**—Include the NAS identifier value (RADIUS attribute 32).
- **order**—Specify the optional values you want to include in the NAS-Port-ID and the customized order in which you want the values to appear. You must include the order option before each optional value (for example, order agent-circuit-id order interface-description).
- **postpend-vlan-tags**—Include the VLAN tags. The router includes the tags in the format :<outer-tag>--<inner-tag> for a double-tagged VLAN, or :<outer-tag> for a single-tagged VLAN.

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

**RELATED DOCUMENTATION**

- Configuring Access Profile Options for Interactions with RADIUS Servers
- Configuring a NAS-Port-ID with Additional Options
- RADIUS Servers and Parameters for Subscriber Access
nas-port-type (Subscriber Management)

Syntax

```
nas-port-type {
  ethernet {
    port-type;
  }
}
```

Hierarchy Level

```
[edit access profile profile-name radius options]
```

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).

NOTE: This statement is ignored if the ethernet-port-type-virtual statement is included in the same access profile.

Default
The router uses a port type of ethernet.

Options

`port-type`—One of the following port types:

- `value`—A value from 0-65535
- `adsl-cap`—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- `adsl-dmt`—Asymmetric DSL, discrete multitone (DMT)
- `async`—Asynchronous
- `cable`—Cable
- `ethernet`—Ethernet
• fddi—Fiber Distributed Data Interface
• g3-fax—G.3 Fax
• hdlc-clear-channel—HDLC Clear Channel
• iapp—Inter-Access Point Protocol (IAPP)
• idsl—ISDN DSL
• isdn-sync—ISDN Synchronous
• isdn-v110—ISDN Async V.110
• isdn-v120—ISDN Async V.120
• piafs—Personal Handyphone System (PHS) Internet Access Forum Standard
• sdsl—Symmetric DSL
• sync—Synchronous
• token-ring—Token Ring
• virtual—Virtual
• wireless—Other wireless
• wireless-1x-ev—Wireless 1xEV
• wireless-cdma2000—Wireless code division multiple access (CDMA) 2000
• wireless-ieee80211—Wireless 802.11
• wireless-umts—Wireless universal mobile telecommunications system (UMTS)
• x25—X.25
• x75—X.75
• xdsl—DSL of unknown type

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

RELATED DOCUMENTATION

| Configuring Access Profile Options for Interactions with RADIUS Servers |
| RADIUS Servers and Parameters for Subscriber Access |
neighbor-discovery-router-advertisement (Access)

Syntax

neighbor-discovery-router-advertisement ndra-pool-name;

Hierarchy Level

[edit access address-assignment]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Configure the name of the address-assignment pool used to assign the router advertisement prefix.

Options
ndra-pool-name—Name of the address assignment pool.

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

RELATED DOCUMENTATION
neighbor-port-info-display

Syntax

```plaintext
neighbor-port-info-display {   
port-description;   
port-id;  
}
```

Hierarchy Level

```
[edit protocols lldp]
```

Release Information

Statement introduced in Junos OS Release 14.1X53-D40 and Release 15.1R5 and Release 16.1R3 for EX Series switches.

Description

Configure the type of Link Layer Discovery Protocol (LLDP) neighbor port information that the switch displays in the Port info field in the output of the `show lldp neighbors` CLI command.

Devices in a network use LLDP to learn about and identify neighbor devices. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices.

The Port info field of the `show lldp neighbors` command displays the port information received from LLDP neighbors. This information is sent from the LLDP neighbor to the switch in a type, length, and value (TLV) message. You can use the `neighbor-port-info-display` CLI statement to configure the switch to display the information contained in either the Port Description TLV or the Port Identification TLV.

By default, the information contained in the Port Description TLV is used for the port information and is displayed in the Port info field. The Port Description TLV contains the textual description of the logical unit or the port. The description for the logical unit is used, if available; otherwise, the description for the physical interface (port) is used. For example, LAG member interfaces do not contain a logical unit; therefore, only the description configured on the physical interface is used.

The Port Identification TLV contains the identifier for the neighbor port. The SNMP index of the interface is used as the port identifier.

Default

On EX Series switches, the Port info field in the output of the `show lldp neighbors` CLI command displays the Port Description TLV.

Options
**port-description**—Configure this option to display the Port Description TLV in the Port info field of the `show lldp neighbors` CLI command.

**port-id**—Configure this option to display the Port Identification TLV in the Port info field of the `show lldp neighbors` CLI command.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>show lldp neighbors</th>
<th>2697</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring LLDP (CLI Procedure)</td>
<td>654</td>
</tr>
<tr>
<td>Understanding LLDP</td>
<td>653</td>
</tr>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
<td>661</td>
</tr>
</tbody>
</table>
netbios-snooping

Syntax

netbios-snooping;

Hierarchy Level

[edit protocols lldp]

Release Information
Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description
Enable NetBIOS snooping on the switch.

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

RELATED DOCUMENTATION

- Configuring NetBIOS Snooping (CLI Procedure) | 670
**next-hop (Dynamic Access Routes)**

**Syntax**

```plaintext
next-hop next-hop;
```

**Hierarchy Level**

```plaintext
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options access route prefix],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name access route prefix],
[edit dynamic-profiles profile-name routing-options access route prefix]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.


**Description**

Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.

The next-hop gateway can be specified explicitly in the framed route, as either the subscriber’s fixed address (common for business subscribers) or 0.0.0.0. Alternatively, the absence of the gateway address implies address 0.0.0.0. The address 0.0.0.0, whether implicit or explicitly configured, resolves to the subscriber’s assigned address (host route).

If the RADIUS Framed-Route attribute (22) or Framed-IPv6-Route attribute [99] does not specify the next-hop gateway—as is common—the variable representing the next-hop automatically resolves to the subscriber’s IP address.

**Options**

`next-hop`—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.

- For IPv4 access routes, use the variable, `$junos-framed-route-nexthop`. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, `$junos-framed-route-ipv6-nexthop`. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].
Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Dynamic Access Routes for Subscriber Management
next-server

Syntax

next-server next-server;

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp pool pool-id],
[edit system services dhcp static-binding mac-address]

Release Information
Statement introduced in Junos OS Release 8.4.

Description
(J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact.

Options

next-server—The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

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

RELATED DOCUMENTATION
no-adaptation

Syntax

no-adaptation;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients  | 869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients  | 862
no-allow-snooped-clients

Syntax

no-allow-snooped-clients;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 10.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Explicitly disable DHCP snooping support on DHCP relay agent.

Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly disable snooping support for DHCPv6 relay agent.

NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Release 10.1 and later, DHCP snooping is disabled by default.

Required Privilege Level

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

RELATED DOCUMENTATION
no-bind-on-request (DHCP Relay Agent)

Syntax

no-bind-on-request;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information

Statement introduced in Junos OS Release 10.4.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (stray requests). Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.
NOTE: Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Extended DHCP Relay Agent Overview | 792
- Overriding the Default DHCP Relay Configuration Settings | 803
- Disabling Automatic Binding of Stray DHCP Requests | 780
no-listen

Syntax

```text
no-listen;
```

Hierarchy Level

```text
[edit forwarding-options helpers bootp interface (interface-name | interface-group)],
[edit forwarding-options helpers domain interface interface-name],
[edit forwarding-options helpers port port-number interface interface-name],
[edit forwarding-options helpers tftp interface interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description

Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring DNS and TFTP Packet Forwarding
- Configuring Port-based LAN Broadcast Packet Forwarding
- Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents
no-mac-table-binding (802.1X)

Syntax

no-mac-table-binding;

Hierarchy Level

[edit protocols dot1x authenticator]

Release Information

Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

For 802.1X authentication, disable the removal of the session from the authentication session table when the MAC address ages out of the Ethernet switching table.

Default

Not enabled

Required Privilege Level

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

RELATED DOCUMENTATION

Controlling Authentication Session Timeouts (CLI Procedure) | 371
no-passwords

Syntax

no-passwords;

Hierarchy Level

[edit system services ssh]

Description

Disable ssh password based authentication.

NOTE: Enabling this option under [edit system services ssh] applies to SSH login service and NETCONF running over ssh services.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring SSH Service for Remote Access to the Router or Switch | 294
no-public-keys

**Syntax**

no-public-keys;

**Hierarchy Level**

[edit system services ssh]
[edit system login user user-name authentication]

**Release Information**

Statement introduced in Junos OS Release 15.1.

**Description**

Disable public key authentication system wide. If you specify the no-public-keys statement at the [edit system login user user-name authentication] hierarchy level, you disable public key authentication for a specific user.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>user</th>
<th>2402</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>2284</td>
</tr>
</tbody>
</table>
no-reauthentication

Syntax

no-reauthentication;

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [interface-names])]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
For 802.1X authentication, disables reauthentication.

Default
Not disabled

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

RELATED DOCUMENTATION

- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Configuring 802.1X Authentication (J-Web Procedure)
- Understanding Authentication on Switches | 361
no-tagging

Syntax

no-tagging;

Hierarchy Level

[edit protocols lldp]

Release Information

Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Configure the switch to send LLDPDUs without including VLAN tags on interfaces for which VLAN tagging in enabled (tagged interfaces).

Default

Interfaces for which VLAN tagging is enabled include a VLAN tag (tag 0) in LLDPDUs if the no-tagging option is not configured.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding LLDP and LLDP-MED on EX Series Switches | 661
no-tcp-forwarding

Syntax

no-tcp-forwarding

Hierarchy Level

[edit system services ssh]

Release Information

Statement introduced in Release 11.4 of Junos OS.

Description

Use this configuration option to prevent a user from creating an SSH tunnel over a CLI session to a Junos router via SSH. This type of tunnel could be used to forward TCP traffic, bypassing any firewall filters or ACLs, allowing access to resources beyond the router.

NOTE: This configuration option does not affect the existing SSH sessions and applies to only the new SSH sessions.

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Configuring SSH Service for Remote Access to the Router or Switch | 294 |
| ssh | 2284 |

Junos OS Security Configuration Guide
no-vlan-interface-name

Syntax

```diff
no-vlan-interface-name;
```

Hierarchy Level

```
[edit forwarding-options dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcpv6 relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcp-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcp-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcp-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcp-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Release Information


**NOTE:** The EX Series switches that support the no-vlan-interface-name statement are the EX4300, EX4600, and EX9200 switches.

Description

When you do not want bridge domain or VLAN tag information, do not include the VLAN ID nor the VLAN interface name (the default) in the circuit or remote ID value in the DHCP option 82 information.

**NOTE:** The no-vlan-interface-name statement is mutually exclusive with the use-interface-description and use-vlan-id statements.

When you configure the no-vlan-interface-name statement only, the format displays only the Layer 3 interface:

```
irb.subunit
```
NOTE: The subunit is required and used to differentiate the interface for remote systems.

When you configure the no-vlan-interface-name and use-interface-description statements, the format displays the IRB interface description:

```
irb_descr
```

If you configure the no-vlan-interface-name and use-interface-description statements, and no description for the IRB interface is found, the format displays the IRB interface name:

```
irb
subunit
```

When you configure the no-vlan-interface-name and include-irb-and-l2 statements, the format displays the Layer 2 logical interface name and the IRB interface name:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

When you configure the no-vlan-interface-name, include-irb-and-l2 and use-interface-name statements, the format displays the Layer 2 interface description and the IRB interface name:

```
l2_descr+irb.subunit
```

If you configure the no-vlan-interface-name, include-irb-and-l2 and use-interface-name statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name and the IRB interface name:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Including a Textual Description in DHCP Options*
- *Using DHCP Relay Agent Option 82 Information* | 739
- *Configuring DHCPv6 Relay Agent Options*
**nonpersistent**

**Syntax**

```
nonpersistent;
```

**Hierarchy Level**

```
[edit accounting-options file filename]
```

**Release Information**

Statement introduced in Junos OS Release 8.3.

**Description**

Store log files used for accounting data in the mfs/var/log directory (located on DRAM) instead of the cf/var/log directory (located on the compact flash drive). This feature is useful for minimizing read/write traffic on the router’s compact flash drive.

**NOTE:** If log files for accounting data are stored on DRAM, these files are lost when you reboot the router. Therefore, you should back up these files periodically.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

Configuring the Storage Location of the File
nonvolatile

Syntax

```plaintext
nonvolatile {
   commit-delay seconds;
}
```

Hierarchy Level

```plaintext
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX, and PTX Series routers and SRX firewalls.

The `commit-delay` statement introduced in Junos OS Release 9.0 for EX Series switches.

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

Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure options for SNMP Set requests.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Commit Delay Timer

  ```plaintext
  commit-delay | 1605
  ```
ntp

Syntax

ntp {
    authentication-key key-number type md5 value password;
    boot-server address;
    broadcast <address> <key key-number> <routing-instance-name routing-instance-name> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    source-address source-address <routing-instance-routing-instance-name>;
    trusted-key [key-numbers ];
}

Hierarchy Level

[edit system]

Release Information

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

Description

Configure NTP on the router or switch. In both standalone and chassis cluster modes, the primary Routing Engine runs the NTP process to get the time from the external NTP server. Although the secondary Routing Engine runs the NTP process in an attempt to get the time from the external NTP server, this attempt fails because of network issues. For this reason, the secondary Routing Engine uses NTP to get the time from the primary Routing Engine.

NOTE: There must be no space in the password for configuring the Network Time Protocol (NTP) authentication-key.

Options

authentication-key—Configure NTP authentication keys so authenticated packets can be sent.
boot-server—Configure the server that NTP queries when the router or switch boots to determine the local date and time.

broadcast—Configure the local router or switch to operate in broadcast mode with the remote system.

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

multicast-client—Configure the local router or switch to listen for multicast messages on the local network.

peer—Configure the local router or switch to operate in symmetric active mode with the remote system at the specified address.

server—Configure the local router or switch to operate in client mode with the remote system

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

• **key key-number**—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address. Range: Any unsigned 32-bit integer.

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

• **routing-instance routing-instance**—(Optional) Routing instance through which the server is reachable.

• **version value**—(Optional) Specify the version number to be used in outgoing NTP packets. Range: 1 through 4. Default: 4.

source-address—A valid IP address configured on one of the router or switch interfaces

trusted-key—Configure the keys you are allowed to use when you configure the local router or switch to synchronize its time with other systems on the network.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Synchronizing and Coordinating Time Distribution Using NTP*
- *NTP Time Synchronization on SRX Series Devices*
- *Configuring the NTP Time Server and Time Services*
object-names

Syntax

```
object-names {
    mib-object-name;
}
```

Hierarchy Level

```
[edit accounting-options mib-profile profile-name]
```

Release Information
Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Specify the name of each MIB object for which MIB statistics are collected for an accounting-data log file.

Options

- **mib-object-name**—Name of a MIB object. You can specify more than one MIB object name.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the MIB Profile
oid

Syntax

```plaintext
oid object-identifier (exclude | include);
```

Hierarchy Level

```plaintext
[edit snmp view view-name]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, OCX switches and SRX devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify an object identifier (OID) used to represent a subtree of MIB objects.

Options
exclude—Exclude the subtree of MIB objects represented by the specified OID.
include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

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

RELATED DOCUMENTATION

- Configuring MIB Views
on-demand-address-allocation

Syntax

```
on-demand-address-allocation;
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name]
```

Release Information

Statement introduced in Junos OS Release 17.3R1.

Description

Enables an address or prefix to be allocated on demand when a dual-stack subscriber session is established. Starting in Junos OS Release 18.1R1, when reauthentication is configured, enables per-family address allocation as each family’s DHCP session is established. In earlier released, applies only to the second family of the dual stack.

**NOTE:** You must configure `on-demand-address-allocation` if you also configure reauthentication for dual-stack, single-session DHCP subscribers. This is true whether you enable reauthentication with the `reauthenticate` statement or the Reauthenticate-On-Renew VSA (26-206).

Required Privilege Level

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

**RELATED DOCUMENTATION**

- Configuring RADIUS Reauthentication for DHCP Subscribers
- RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers
- Single-Session DHCP Dual-Stack Overview
operation

Syntax

```
operation operation-name;
```

Hierarchy Level

```
[edit accounting-options mib-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the name of the operation used to collect MIB statistics for an accounting-data log file.

Options

- `operation-name`—Name of the operation to use. You can specify a `get`, `get-next`, or `walk` operation.

  Default: `walk`

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the MIB Profile
option (DHCP server)

Syntax

```plaintext
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Release Information

Description
Configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

Options

- **id-number**—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- **option-type**—Any of the following types: byte, byte-stream, flag, integer, ip-address, short, string, unsigned-integer, unsigned-short.
- **array**—An option can include an array of values.
- **option-value**—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

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

RELATED DOCUMENTATION
Creating User-Defined DHCP Options Not Included in the Default Junos Implementation of the DHCP Server | 707
option-60 (DHCP Local Server)

Syntax

```
option-60;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level

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

RELATED DOCUMENTATION

Using External AAA Authentication Services with DHCP | 833
option-60 (DHCP Relay Agent)

Syntax

```plaintext
option-60 {
  default-action {
    drop drop;
    forward-only forward-only;
    local-server-group local-server-group;
  }
  equals {
    ascii name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
    hexadecimal name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
  }
  not-present {
    drop drop;
    forward-only forward-only;
    local-server-group local-server-group;
  }
  equals {
    ascii name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
    hexadecimal name {
      drop drop;
      forward-only forward-only;
      local-server-group local-server-group;
    }
  }
}
```

Hierarchy Level
[edit bridge-domains name forwarding-options dhcp-relay group name relay-option],
[edit bridge-domains name forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay group name relay-option],
[edit forwarding-options dhcp-relay relay-option],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay relay-option],
[edit logical-systems name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name forwarding-options dhcp-relay relay-option],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay relay-option],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay relay-option],
[edit logical-systems name vlans name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name vlans name forwarding-options dhcp-relay relay-option],
[edit logical-systems name vlans name forwarding-options dhcp-relay relay-option],
[edit logical-systems name vlans name forwarding-options dhcp-relay relay-option],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay group name relay-option],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay relay-option],
[edit routing-instances name forwarding-options dhcp-relay group name relay-option],
[edit routing-instances name forwarding-options dhcp-relay relay-option],
[edit routing-instances name vlans name forwarding-options dhcp-relay group name relay-option],
[edit routing-instances name vlans name forwarding-options dhcp-relay relay-option],
[edit routing-instances name vlans name forwarding-options dhcp-relay relay-option],
[edit vlans name forwarding-options dhcp-relay group name relay-option],
[edit vlans name forwarding-options dhcp-relay relay-option]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement updated in Junos OS Release 17.4R1 for MX Series.

Description
Specify that the payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication or client authentication process.

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

Using External AAA Authentication Services with DHCP | 833

DHCPv4 and DHCPv6 Forward-Only Action for Relay Traffic with Unknown DHCP Server Address
option-82 (DHCP Local Server Authentication)

Syntax

```plaintext
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

```plaintext
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

Options
circuit-id—(Optional) Agent Circuit ID suboption (suboption 1).
remote-id—(Optional) Agent Remote ID suboption (suboption 2).

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

RELATED DOCUMENTATION

Using External AAA Authentication Services with DHCP | 833
option-82 (DHCP Local Server Pool Matching)

Syntax

```plaintext
option-82;
```

Hierarchy Level

```plaintext
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the `ip-address-first` statement before configuring the `option-82` statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 891
- Extended DHCP Local Server Overview | 718
- Address-Assignment Pools Overview
option-82 (DHCP Relay Agent)

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the option 82 that is concatenated with the username during the subscriber authentication or client authentication process. You can specify either, both, or neither the Agent Circuit ID and the Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If neither suboption is supplied, the raw payload of option 82 is concatenated to the username.

NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

Options

circuit-id—(Optional) The string for the Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) The string for the Agent Remote ID suboption (suboption 2).
Required Privilege Level

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

RELATED DOCUMENTATION

Using External AAA Authentication Services with DHCP | 833
option-number (DHCP Relay Agent Option)

Syntax

```
option-number option-number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay dhcpv6 relay-option],
[edit forwarding-options dhcp-relay group group-name relay-option],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Specify the DHCP option DHCP relay agent uses for selective processing of client traffic. You can configure support globally or for a named group of interfaces. You can also configure support for the extended DHCP relay agent on a per logical system and per routing instance basis.

Use the [edit forwarding-options dhcp-relay dhcpv6] hierarchy level to configure the DHCPv6 relay agent support.

Options

- **option-number**—The DHCP or DHCPv6 option in the incoming traffic.

  NOTE: EX Series switches do not support the User Class Options.

- 15 (DHCPv6 only)—Use DHCPv6 option 15 (User Class Option) in packets
- 16 (DHCPv6 only)—(MX Series routers and EX Series switches only) Use DHCPv6 option 16 (Vendor Class Option) in packets
- 60 (DHCPv4 only)—(MX Series routers and EX Series switches only) Use DHCP option 60 (Vendor Class Identifier) in DHCP packets
• 77 (DHCPv4 only)—Use DHCP option 77 (User Class Identifier) in packets

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

**RELATED DOCUMENTATION**

*Using DHCP Option Information to Selectively Process DHCP Client Traffic*
options (Access Profile)

Syntax

options {
    accounting-session-id-format (decimal | description);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    chap-challenge-in-request-authenticator;
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    access-loop-id-local;
    interface-description-format {
        exclude-adapter;
        exclude-channel;
        exclude-sub-interface;
    }
    ip-address-change-notify message;
    juniper-access-line-attributes;
    nas-identifier identifier-value;
    nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
        atm {
            adapter-width width;
            port-width width;
            pw-width width;
            slot-width width;
            vci-width width;
            vpi-width width;
        }
    }
    nas-port-id-delimiter delimiter-character;
nas-port-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  interface-text-description;
  nas-identifier;
  order {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    interface-text-description;
    nas-identifier;
    postpend-vlan-tags;
  }
  postpend-vlan-tags;
}

nas-port-type {
  ethernet {
    port-type;
  }
}

override {
  calling-station-id remote-circuit-id;
  nas-ip-address tunnel-client-gateway-address;
  nas-port tunnel-client-nas-port;
  nas-port-type tunnel-client-nas-port-type;
}

remote-circuit-id-delimiter;
remote-circuit-id-fallback;
remote-circuit-id-format {
  agent-circuit-id;
  agent-remote-id;
}

revert-interval interval;

service-activation {
  dynamic-profile (optional-at-login | required-at-login);
  extensible-service (optional-at-login | required-at-login);
}

vlan-nas-port-stacked-format;

Hierarchy Level

[edit access profile profile-name radius]
Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
juniper-dsl-attributes introduced in Junos OS Release 11.4.
remote-circuit-id-delimiter, remote-circuit-id-fallback, and remote-circuit-id-format introduced in Junos OS Release 13.3R1 on MX Series.
nas-identifier introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.
service-activation introduced in Junos OS Release 16.2.

Description
Configure the options used by RADIUS authentication and accounting servers.
Options

accounting-session-id-format—(EX Series, MX Series only) Configure the format the router or switch uses to identify the accounting session. The default is decimal.

Values:
- decimal—Use the decimal format.
- description—Use the generic format, in the form: `jnpr interface-specifier:subscriber-session-id`.

calling-station-id-delimiter—(MX Series, T Series only) Starting in Junos OS Release 13.1, specify the character that the router uses as a separator between the concatenated values in the Calling-Station-ID (RADIUS IETF attribute 31) string. The router uses the delimiter when you configure more than one value in the calling-station-id-format statement. The default is the hash (#) character.

Values:
- delimiter-character—Character to use for the delimiter. You must enclose the delimiter character in quotation marks (" ").

chap-challenge-in-request-authenticator—(MX Series only) Starting in Junos OS Release 15.1, configure the authd process to insert the random challenge generated by the NAS into the Request Authenticator field of Access-Request packets, if the challenge value is 16 bytes long. If you enable the chap-challenge-in-request-authenticator statement and the random challenge is not 16 bytes long, authd ignores the statement and uses the default behavior, which inserts the random challenge as the CHAP-Challenge attribute (RADIUS attribute 60) in Access-Request packets.

client-accounting-algorithm—(EX Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the access method the router uses to access RADIUS accounting servers. The default is the direct option.

Values:
- direct—Use the direct method.
- round-robin—Use the round-robin method.

client-authentication-algorithm—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, configure the method that the authenticator uses to access RADIUS authentication servers when there are multiple servers configured. Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The router or switch, acting as the authenticator, waits for a response from the server before sending another request.

When there are multiple RADIUS server connections configured for a client, the authenticator attempts to reach the different servers in the order that they are configured. If there is no response from the first RADIUS server, the authenticator attempts to reach the next RADIUS server. This process repeats until the client is either granted access or there are no more configured servers.

If the direct method is configured, the authenticator always treats the first server in the list as the primary server. The authenticator moves on to the second server only if the attempt to reach the first
server fails. If the **round-robin** method is configured, the server chosen first will be rotated based on which server was used last. The first server in the list is treated as a primary for the first authentication request, but for the second request, the second server configured is treated as primary, and so on. With this method, all of the configured servers receive roughly the same number of requests on average so that no single server has to handle all of the requests.

**NOTE:** The **round-robin** access method is not recommended for use with EX Series switches.

**Default:** The default is the **direct** option.

**Values:**

- **direct**—Use the direct access method. The authenticator contacts the first RADIUS server on the list for each request, the second server if the first one fails, and so on.
- **round-robin**—Use the round-robin method. The authenticator contacts the first RADIUS server for the first request, the second server for the second request, and so on.

**coa-dynamic-variable-validation**—(EX Series, M Series, MX Series only) Starting in Junos OS Release 13.2X50-D10 for EX Series switches, specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

**Default:** If you do not configure this statement, the router does not apply any incorrect variable updates, but does make any other changes to the client profile dynamic variables, and responds with an ACK message.

**ethernet-port-type-virtual**—(EX Series, M Series, MX Series only) Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of **ethernet** in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of **virtual**.

**NOTE:** This statement takes precedence over the **nas-port-type** statement if you include both statements in the same access profile.
**access-loop-id-local**—Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

**ip-address-change-notify**—(MX Series only) Starting in Junos OS Release 13.1, for on-demand address allocation for dual-stack PPP subscribers, specify that the BNG includes the IPv4-Release-Control VSA (26–164) in the Access-Request that is sent during on-demand IP address allocation and in the Interim-Accounting messages that are sent to report an address change. The configuration of this statement has no effect when on-demand IP address allocation or deallocation is not configured.

Optionally, configure a message that is included in the VSA when it is sent to the RADIUS server.

**Default:** This functionality is disabled by default.

**Values:**
- **message**—VSA message.

**Range:** Up to 32 characters.

**juniper-access-line-attributes**—Configure AAA to add Juniper Networks access line VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:

- **Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)**—Default configured advisory transmit speed.
- **Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)**—Default configured advisory receive speed.

**NOTE:** Starting in Junos OS Release 19.2R1, the **juniper-access-line-attributes** option replaces the **juniper-dsl-attributes** option. The difference between these options is that **juniper-dsl-attributes** supported only DSL TLVs received in the ANCP Port Status message. The **juniper-access-line-attributes** option supports PON TLVs in addition to DSL TLVs, and will be extensible to future access technologies.

For backward compatibility with existing scripts, the **juniper-dsl-attributes** option redirects to the new **juniper-access-line-attributes** option. We recommend that you use **juniper-access-line-attributes**.

**Default:** The Juniper Networks access line VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.
nas-identifier—(EX Series, MX Series, SRX Series only) Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests. This statement was introduced in Junos OS Release 15.1X49-D110 for SRX300, SRX320, SRX340, SRX345, and SRX550M Series devices.

Values: identifier-value—String to use for authentication and accounting requests.

Range: 1 through 64 characters.

nas-port-id-delimiter—(MX Series only) Starting in Junos OS Release 11.4, specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the nas-port-id-format statement. The default is the hash (#) character. This statement was introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Values: delimiter-character—Character used for the delimiter.

remote-circuit-id-delimiter—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure a delimiter character for the remote circuit ID string when you use the remote-circuit-id-format statement to configure the string to use instead of the Calling-Station ID in L2TP Calling Number AVP 22. If more than one value is configured for the remote circuit ID format, the delimiter character is used as a separator between the concatenated values in the resulting remote circuit ID string. The default is the hash (#) character.

Values: delimiter—Delimiter character to be used between components of the remote circuit ID string.

remote-circuit-id-fallback—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the fallback value for the LAC to send in L2TP Calling Number AVP 22, either the configured Calling-Station-ID or the default underlying interface. Use of the fallback value is triggered when the components of the override string you configured with the remote-circuit-id-format statement—the ACI, the ARI, or both ACI and ARI—are not received by the LAC in the PPPoE Active Discovery Request (PADR) packet.

Values:

- configured-calling-station-id—Send the configured Calling-Station-ID in the Calling Number AVP.
- default—Send the underlying interface value in the Calling Number AVP.
remote-circuit-id-format—(MX Series only) Starting in Junos OS Release 13.3R1 on MX Series, configure the format of the string that overrides the Calling-Station-ID format in the Calling Number AVP 22 sent by the LAC to the LNS in the ICRQ packet when an L2TP session is being established. You can specify the ACI, the ARI, or both the ACI and ARI. This statement enables you to decouple the AVP 22 value from the RADIUS Calling-Station-ID attribute (31); the values for AVP 22 and the Calling-Station-ID attribute are the same when you use the calling-station-id-format statement to configure AVP 22.

NOTE: You must configure the override calling-circuit-id remote-circuit-id statement for the remote circuit ID format to be used in the calling number AVP.

Values:

- **agent-circuit-id**—Specifies use of the ACI string that uniquely identifies the subscriber’s access node and the digital subscriber line (DSL) on the access node. For PPPoE traffic, the ACI string is in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) control packets.

- **agent-remote-id**—Specifies use of the ARI string that identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The agent remote identifier (ARI) string is stored in the DSL Forum Agent-Remote-ID VSA [26-2] for PPPoE traffic.
service-activation—(MX Series only) Starting in Junos OS Release 16.2, specify whether subscribers are allowed to log in even when service activation failures related to configuration errors occur during family activation request processing by authd for a newly authenticated subscriber. Configuration errors include missing or incorrect syntax, missing or incomplete references to dynamic profiles, and missing or incomplete variables.

NOTE: This configuration does not apply to services activated by means of RADIUS CoA requests, JSRC Push-Profile-Request (PPR) messages, or subscriber secure policies.

You can enable separate configurations for subscriber login services for two service-activation types: dynamic-profile and extensible-service. You configure the dynamic-profile type services in the dynamic profile at the [edit dynamic-profiles] hierarchy level; the profile is used to provide dynamic subscriber access and services for broadband applications. The extensible-service type is for business services configured in an operation script and provisioned by the Extensible Subscriber Services Manager daemon (essmd).

Default:
Default behavior depends on the service type:

- For extensible-service services: optional-at-login.
- For dynamic-profile services: required-at-login.

Values:
- optional-at-login—Service activation is optional. Failure due to configuration errors does not prevent activation of the address family; it allows subscriber access. Failure for any other reason causes network family activation to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.
- required-at-login—Service activation is required. Failure for any reason causes the Network-Family-Activate-Request for that network family to fail. If no other network family is already active for the subscriber, then the client application logs out the subscriber.

vlan-nas-port-stacked-format—(MX Series only) Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

Configuring Access Profile Options for Interactions with RADIUS Servers

RADIUS Servers and Parameters for Subscriber Access

Configuring Authentication and Accounting Parameters for Subscriber Access

Configuring a Calling-Station-ID with Additional Options
options (Security)

Syntax

options (basic | isis-enhanced);

Hierarchy Level

[edit security authentication-key-chains key-chain key-chain-name key key]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

For IS-IS only, configure the protocol transmission encoding format for encoding the message authentication code in routing protocol packets.

Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.

Options

basic—RFC 5304 based encoding. Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.

isis-enhanced—RFC 5310 based encoding. Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.

Default: basic

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring Hitless Authentication Key Rollover for IS-IS

Understanding Hitless Authentication Key Rollover for IS-IS
order

Syntax

```
order (radius | [ accounting-order-data-list ]);  
```

Hierarchy Level

```
[edit access profile profile-name accounting]  
```

Release Information

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

Description

Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending accounting messages and updates.

Default

No order specified

Options

radius—RADIUS accounting for specified subscribers.

[ accounting-order-data-list ]— Set of data listing the authentication order to be used, enclosed by brackets. This can be any combination of the authentication methods, up to and including a full list of the entire authentication order.

NOTE: The [edit access] hierarchy is not available on QFabric systems.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
outbound-ssh

Syntax

```conf
outbound-ssh {
  client client-id {
    address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    routing-instance routing-instance-name
      secret password;
      services netconf;
    }
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
`routing-instance` option introduced in Junos OS Release 19.3R1 for SRX Series and MX Series devices.

Description

Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.

Default
To configure transmission of the router’s or switch’s device ID to the application, include the `device-id` statement at the [edit system services] hierarchy level.
Options

client-id—Identifies the outbound-ssh configuration stanza on the router or switch. Each outbound-ssh stanza represents a single outbound SSH connection. This attribute is not sent to the client.

device-id—Identifies the router or switch to the client during the initiation sequence.

keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the timeout and retry attributes.

reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:

- in-order—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.

- sticky—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

routing-instance routing-instance-name—(SRX Series and MX Series only) Specify the name of the routing instance on which the outbound SSH connectivity needs to be established. If you do not specify a routing instance, your device will establish the outbound SSH connection using the default routing table.

secret—(Optional) Router’s or switch’s public SSH host key. If added to the outbound-ssh statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router’s or switch’s public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the retry and timeout values for each client listed.

address—Hostname, IPv4 address, or IPv6 address of the NSM application server. You can list multiple clients by adding each client’s IP address or hostname along with the following connection parameters:

- port—Outbound SSH port for the client. The default is port 22.

- retry—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
• **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

**NOTE:** Starting in Release 15.1, Junos OS supports outbound SSH connections with devices having IPv6 addresses.

---

**filename**—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, mib2d or snmpd). Use this option to override the default value.

**files**—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

**size**—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

**match**—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to =error, the system only records lines to the trace file that include the string error.

**services**—Services available for the session. Currently, NETCONF is the only service available.

**world-readable | no-world-readable**—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (no-world-readable).

**all | configuration | connectivity**—(Optional) Type of tracing operation to perform.

**all**—Log all events.

**configuration**—Log all events pertaining to the configuration of the router or switch.

**connectivity**—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

**no-remote-trace**—(Optional) Disable remote tracing.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
outbound-ssh

Syntax

```plaintext
outbound-ssh {
  client client-id {
    address address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    routing-instance routing-instance-name
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Support for IPv6 address added in Junos OS Release 12.1X47-D15.
`routing-instance` option introduced in Junos OS Release 19.3R1 for SRX Series and MX Series devices.

Description

Initiate outbound SSH connections.

Options
client client-id—Defines a device-initiated connection. This value serves to uniquely identify the outbound-ssh configuration stanza. Each outbound-ssh stanza represents a single outbound SSH connection. Thus, the administrator is free to assign the client-id any meaningful unique value.

address address—Specifies the IPv4 or IPv6 address or hostname of the client.

port port-number—Specifies the port at which a server listens for outbound SSH connection requests.

retry number—Specifies the maximum number of connection attempts a device can make to the specified IP address. The default is three attempts.

timeout seconds—Specifies how long the application waits between attempts to reconnect to the specified IP address, in seconds. The default is 15 seconds.

device device-id—Identifies the device to the management client. Each time the device establishes an outbound SSH connection, it first sends an initiation sequence (device-id) to the management client.

keep-alive—Enables the device to send SSH protocol keepalive messages to the client application. The timeout statement specifies how long the device waits to receive data before sending a request for acknowledgment from the application. The default is 15 seconds. The retry statement specifies how many keepalive messages the router sends without receiving a response from the client. When that number is exceeded, the device disconnects from the application, ending the outbound SSH connection. The default is three retries.

reconnect-strategy (in-order|sticky)—Specifies how the device reconnects to the server after a connection is dropped.

in-order—Configures the device to reconnect to the first configured server. If this server is unavailable, the device tries to connect to the next configured server. This process repeats until a connection is completed.

sticky—Configures the device to reconnect to the server from which it disconnected.

routing-instance routing-instance-name—(SRX Series and MX Series only) Specify the name of the routing instance on which the outbound SSH connectivity needs to be established. If you do not specify a routing instance, your device will establish the outbound SSH connection using the default routing table.

secret password—Sends the device’s public SSH host key when the device connects to the client.

services netconf—Configures the application to accept NETCONF as an available service.

Required Privilege Level

system—To view this statement in the configuration.

system-control—to add this statement to the configuration.
RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>traceoptions (Outbound SSH)</th>
<th>2356</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Outbound SSH Service</td>
<td>306</td>
</tr>
</tbody>
</table>


overrides (DHCP Local Server)

Syntax

```plaintext
asymmetric-lease-time seconds;
asymmetric-prefix-lease-time seconds;
client-discover-match <option60-and-option82 | incoming-interface>;
client-negotiation-match incoming-interface;
delay-advertise {
based-on (option-15 | option-16 | option-18 | option-37) {
equals {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
not-equals {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
starts-with {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
}
delay-time seconds;
}
delay-offer {
based-on (option-60 | option-77 | option-82) {
equals {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
not-equals {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
starts-with {
ascii ascii-string;
hexadecimal hexadecimal-string;
}
}
delay-time seconds;
}
delegated-pool;
delete-binding-on-renegotiation;
```
dual-stack dual-stack-group-name;
include-option-82 {
  forcerenew;
  nak;
}
interface-client-limit number;
multi-address-embedded-option-response;
process-inform {
  pool pool-name;
}
protocol-attributes attribute-set-name;
rapid-commit;
}

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information
Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support for the allow-no-end option introduced in Junos OS Release 14.1X53-D15 for EX Series switches.
Statement introduced in Junos OS Release 12.3X48-D10 for SRX Series devices.
Description
Override the default configuration settings for the extended DHCP local server. Specifying the `overrides` statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the `overrides` statement and its subordinate statements at the `[edit system services dhcp-local-server]` hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group group-name]` hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group group-name interface interface-name]` hierarchy level.
- Use the `[edit system services dhcp-local-server dhcpv6]` hierarchy level to override DHCPv6 configuration options.

**NOTE:** By default, `jdhcp` does not process DHCPINFORM message. Only after you enable the `overrides` command using the `set system services dhcp-local-server overrides process-inform` statement, `jdhcp` starts processing the DHCPINFORM message.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

The `interface-client-limit` statement is not supported in the `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

The `asymmetric-prefix-lease-time`, `delegated-pool`, `multi-address-embedded-option-response`, and `rapid-commit` statements are supported in the `[edit system services dhcp-local-server dhcpv6 ...]` hierarchy level only.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Extended DHCP Local Server Overview</th>
<th>718</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overriding the Default DHCP Local Server Configuration Settings Overview</td>
<td>807</td>
</tr>
<tr>
<td>Configuring a DHCP Server on Switches (CLI Procedure)</td>
<td>759</td>
</tr>
</tbody>
</table>
overrides (DHCP Relay Agent)

Syntax

overrides {
  allow-no-end-option;
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match <option60-and-option82 | incoming-interface>;
  client-negotiation-match incoming-interface;
  delay-authentication;
  delete-binding-on-renegotiation;
  disable-relay;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  relay-source
  replace-ip-source-with;
  send-release-on-delete;
  trust-option-82;
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**
Override the default configuration settings for the extended DHCP relay agent. Specifying the `overrides` statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

The following statements are supported at both the [edit ... dhcp-relay] and [edit ... dhcpv6] hierarchy levels.

- `allow-snooped-clients`
- `asymmetric-lease-time`
- `delete-binding-on-renegotiation`
- `dual-stack`
- `interface-client-limit`
- `no-allow-snooped-clients`
- `no-bind-on-request`
- `relay-source`
- `send-release-on-delete`

The following statements are supported at the [edit ... dhcpv6] hierarchy levels only.

- `asymmetric-prefix-lease-time`

All other statements are supported at the [edit ... dhcp-relay] hierarchy levels only.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**
- Extended DHCP Relay Agent Overview | 792
- Overriding the Default DHCP Relay Configuration Settings | 803
overrides (DHCP Relay Agent)

Syntax

overrides {
    allow-no-end-option;
    always-write-option-82;
    asymmetric-lease-time;
    bootp-support;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack;
    no-bind-on-request;
    relay-source;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
    user-defined-option-82;
}

Hierarchy Level

[edit forwarding-options dhcp-relay]

Release Information
Statement introduced in Junos OS Release 15.1X49-D100.

Description
Override the default configuration settings for the extended DHCP relay agent. Specifying the overrides statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level.

Options
allow-no-end-option—Accept packets without end-of-option.

asymmetric-lease-time—Provides a way to send the DHCP client a lease that is shorter than the actual lease granted by the DHCP local server.

Range: 600 through 86,400 seconds.

bootp-support—Allows send bootp request from a remote client to a DHCP server for an IP address.

delete-binding-on-renegotiation—Allows DHCP relay agent to delete binding information for a specific client when a DHCP DISCOVER packet is received from the client.

disable-relay—Disable DHCP relay processing.
**dual-stack**—Specify the dual stack group to use.

**no-bind-on-request**—Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (stray requests).

**relay-source**—Specify the interface for relay source.

**send-release-on-delete**—Always send RELEASE to the server when a binding is deleted.

**trust-option-82**—Allow processing of DHCP client packets that have a gateway IP address giaddr of 0 and contain option 82 information.

**user-defined-option-82**—Specify user defined description for option-82.

The remaining statements are explained separately. see CLI Explorer.

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

| replace-ip-source-with (DHCP Relay Agent) | 2192 |
| always-write-option-82 | 1499 |
overrides (System Services DHCP)

Syntax

```yaml
overrides {
    interface-client-limit number;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server dhcpv6 group group-name]
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]
```

Release Information
Statement introduced in Junos OS Release 10.4.

Description
Override the default configuration settings for the extended DHCP local server. Specifying the `overrides` statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the `overrides` statement and its subordinate statements at the `[edit system services dhcp-local-server]` hierarchy level.
- To override configuration options for a named group of interfaces, include the statements at the `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.
- To override configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]` hierarchy level.
- Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.

Options

- **interface-client-limit number**—Sets the maximum number of DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Range: 1 through 500,000

Default: No limit

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

Syntax

```plaintext
password {
    change-type (set-transitions | character-set);
    format (sha1 | sha256 | sha512);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
```

Hierarchy Level

```plaintext
[edit system login]
```

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION
password (Access Control Service)

Syntax

```powershell
password password;
```

Hierarchy Level

```powershell
[edit services unified-access-control infranet-controller hostname]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the password to connect the switch to the Junos Pulse Access Control Service network access control (NAC) device. This password must match the password specified on the Access Control Service though its administrative interface.

Options

- `password`—A string of up to 200 alphanumeric characters bounded by quotation marks. Spaces are allowed, but special characters, such as ?, are not allowed.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
password (DHCP Local Server)

Syntax

password password-string;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name authentication],
[edit system services dhcp-local-server group group-name authentication]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

**Options**

*password-string*—Authentication password.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Using External AAA Authentication Services with DHCP | 833
password (DHCP Relay Agent)

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name authentication] hierarchy level introduced in Junos OS Release 15.1.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or client authentication. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options
password-string—Authentication password.

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

RELATED DOCUMENTATION

- Using External AAA Authentication Services with DHCP | 833
- Configuring Passwords for Usernames
password (Login)

Syntax

```plaintext
password {
    change-type (set-transitions | character-set);
    format (sha1 | sha256 | sha512);
    minimum-character-changes number
    maximum-length length;
    maximum-lifetime days
    minimum-changes number;
    minimum-length length;
    minimum-lifetime days
    minimum-lower-cases number;
    minimum-numerics number;
    minimum-punctuations number;
    minimum-reuse number;
    minimum-upper-cases number;
}
```

Hierarchy Level

[edit system login]

Release Information

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

Description

Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

Using several password minimum requirement options will cause the minimum-length to be reset if the total sum of the required minimums exceeds the minimum-length setting.

The individual statements are explained separately.

Required Privilege Level

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

Syntax

password-options {
  apply-groups;
  apply-groups-except;
  tacplus-authorization;
}

Hierarchy Level

[edit system]

Release Information
Statement introduced in Junos OS Release 19.3R1 on MX Series routers.
Option tacplus-authorization introduced in Junos OS Release 19.3R1 on MX Series routers.

NOTE: You must configure password under authentication-order when password-options is configured.

Description
Configure options for local authentication.

Options
apply-groups—Choose the groups from which to inherit configuration data.
apply-groups-except—Choose the groups to be excluded from configuration data being inherited.
tacplus-authorization—Choose the remote authorization for locally authenticated users.

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

RELATED DOCUMENTATION
path-length

Syntax

```
path-length certificate-path-length;
```

Hierarchy Level

```
[edit security certificates]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on MSeries and TSeries routers and EX Series switches only) Configure the digital certificate path length.

Options

- `certificate-path-length`—Digital certificate path length.

Range: 2 through 15 certificates

Default: 15 certificates

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Path Length for the Certificate Hierarchy
partition (Gx-Plus)

Syntax

```
partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm;
}
```

Hierarchy Level

```
[edit access gx-plus]
```

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure a Gx-Plus partition.

Options

* partition-name — Name of the Gx-Plus partition.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Gx-Plus
- Configuring the Gx-Plus Partition
peer (NTP)

Syntax

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

Hierarchy Level

```
[edit system ntp]
```

Release Information
Statement introduced before Junos OS Release 7.4.

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

Options

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

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

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

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

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

  **Range:** 1 through 4

  **Default:** 4

Required Privilege Level

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

RELATED DOCUMENTATION

- ntp | 2005
pool (DHCP Local Server Overrides)

Syntax

pool pool-name;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides process-inform],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcv6 overrides process-inform],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcv6 group group-name overrides process-inform],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcv6 group group-name interface interface-name overrides process-inform],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name overrides process-inform],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name interface interface-name overrides process-inform],
[edit logical-systems logical-system-name system services dhcp-local-server dhcv6 group group-name interface interface-name overrides process-inform],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides process-inform],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name interface interface-name overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcv6 overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcv6 group group-name overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcv6 group group-name interface interface-name overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name overrides process-inform],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name interface interface-name overrides process-inform],
[edit system services dhcp-local-server overrides process-inform],
[edit system services dhcp-local-server dhcv6 overrides process-inform],
[edit system services dhcp-local-server dhcv6 group group-name overrides process-inform],
Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure DHCP or DHCPv6 local server to reply to DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) with information taken from the specified pool without interacting with AAA.

Options
pool-name—Name of the address pool, which must be configured within family inet for DHCP local server and within family inet6 for DHCPv6 local server.

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

RELATED DOCUMENTATION
- Enabling Processing of Client Information Requests | 839
- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
pool (System)

Syntax

```
pool address/prefix-length {
  address-range {
    low address;
    high address;
  }
  exclude-address {
    address;
  }
}
```

Hierarchy Level

```
[edit system services dhcp],
```

Release Information

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

Description

For J Series Services Routers and EX Series switches only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.

Options

- **address-range**—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

- **exclude-address**—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION
pool-match-order

Syntax

```
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1.

Description

Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Default

DHCP local server uses the `ip-address-first` method to determine which address pool to use.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 891
- Extended DHCP Local Server Overview | 718
port (Access Control Service)

Syntax

```plaintext
port port-number;
```

Hierarchy Level

```
[edit services unified-access-control infranet-controller]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the switch's connection to the security port on the Junos Pulse Access Control Service network access control (NAC) device.

**NOTE:** Do not change this port setting.

Options

- `port-number—11123`

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
**port (HTTP/HTTPS)**

**Syntax**

```
port port-number;
```

**Hierarchy Level**

```
[edit system services web-management]
```

**Release Information**

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

**Description**

Configure the port on which the HTTP or HTTPS service is connected.

**Options**

`port-number`—The TCP port number on which the specified service listens.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Secure Management Access Configuration Summary
- J-Web Interface User Guide
  - http | 1838
  - https | 1839
  - web-management | 2431
port (NETCONF)

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit system services netconf]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Configure the TCP port used for NETCONF-over-SSH connections.

NOTE:

- The configured port accepts only NETCONF-over-SSH connections. Regular SSH session requests for this port are rejected.
- The default SSH port (22) continues to accept NETCONF sessions even with a configured NETCONF server port. To disable the SSH port from accepting NETCONF sessions, you can specify this in the login event script.
- We do not recommend configuring the default ports for FTP (21) and Telnet (23) services for configuring NETCONF-over-SSH connections.

Options

```
port port-number—Port number on which to enable incoming NETCONF connections over SSH.
```

Default: 830 (as specified in RFC 4742, *Using the NETCONF Configuration Protocol over Secure Shell (SSH)*)

Range: 1 through 65535

Required Privilege Level

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

RELATED DOCUMENTATION

- *NETCONF XML Management Protocol Guide*
port (RADIUS Server)

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit system radius-serveraddress],
[edit system accounting destination radius server address]
```

Release Information

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

Description

Configure the port number on which to contact the RADIUS server.

Options

- `number`—Port number on which to contact the RADIUS server.

Default: 1812 (as specified in RFC 2865)

NOTE: The [edit system accounting] hierarchy is not available on QFabric systems.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
port (SRC Server)

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit system services service-deployment servers server-address]
```

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

Description
Configure the port number on which to contact the SRC server.

Options

- `port-number`—(Optional) The TCP port number for the SRC server.

Default: 3333

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Junos OS to Work with SRC Software
port (TACACS+ Server)

**Syntax**

```
port port-number;
```

**Hierarchy Level**

```
[edit system accounting destination tacplus server server-address]
```

**Release Information**

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

**Description**

Configure the port number on which to contact the TACACS+ server.

**Options**

- `number`—Port number on which to contact the TACACS+ server.

**Default:** 49

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring TACACS+ System Accounting | 278
port-description-type

Syntax

```plaintext
port-description-type {
  interface-alias;
  interface-description;
}
```

Hierarchy Level

```plaintext
[edit protocols lldp]
[edit routing-instances routing-instance-name protocols lldp]
```

Release Information

Statement introduced in Junos OS Release 13.3R5, 14.2R2, 14.1R4, and 12.3R9.

Description

For Link Layer Discovery Protocol, configure the value to be used for port description TLV.

Options

- `interface-alias`—Use the `ifAlias` MIB object value to generate the port description TLV.
- `interface-description`—Use the `ifDescr` MIB object value to generate the port description TLV.

Default: By default, `interface-alias` is used for generation of port description TLV. The `interface-alias` value is same as description of an interface configured by statement `set interface name description description`.

NOTE: The LLDP MIB `lldpLocPortDesc` value gets changed depending on the setting of `port-description-type` statement. That is:

- If you configure the `port-description-type interface-alias` statement, the MIB variable `lldpLocPortDesc` displays the value same as that of MIB variable `ifAlias`, which is same as the description of the interface. By default, the MIB variable `lldpLocPortDesc` displays the value same as that of MIB variable `ifAlias`.

- If you configure the `port-description-type interface-description` statement, the MIB variable `lldpLocPortDesc` displays the value of MIB variable `ifDescr`, which is same as that of interface name.

Required Privilege Level

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

RELATED DOCUMENTATION

```
lldp | 1900

show lldp

show lldp neighbors
```
**port-id-subtype**

**Syntax**

```plaintext
port-id-subtype {
    interface-name;
    locally-assigned;
}
```

**Hierarchy Level**

```plaintext
[edit protocols lldp]
[edit routing-instances routing-instance-name protocols lldp]
```

**Release Information**

Statement introduced in Junos OS Release 12.3R1

**Description**

For Link Layer Discovery Protocol, configure the port ID type, length, and value (TLV).

**Options**

- `interface-name`—Use the interface name to generate the port ID TLV.

**Default:** Use the SNMP index of the interface to generate the port ID TLV. This is the default option used to generate port ID TLV.

**NOTE:** For QFX5200 switches, the default value used to generate port ID TLV in LLDP messages is interface name, not SNMP index.

**NOTE:** The `show lldp neighbors` command displays the content of the port ID TLV received from the peer in the **port Info** field. Changing the configuration of `port-id-subtype` affects the display of the `show lldp neighbors` command on the peer device running Junos OS.

When the value of **port-id-subtype** is set to **locally-assigned**, which is the default value, the `show lldp neighbors` command on the peer device running Junos OS displays the SNMP index as the port information for the local device.

When the value of **port-id-subtype** is set to **interface-name**, the `show lldp neighbors` command on the peer device running Junos OS displays the interface name as the port information for the local device.
The value of the MIB variable instance `lldpLocPortId` depends on the entity that is used to generate the port ID TLV. If the port ID TLV generation is configured to use the interface-name in the command `set port-id-subtype interface-name`, then the value of the MIB variable `lldpLocPortId` instance is the interface name and not the SNMP index.

**Required Privilege Level**

routing—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- `lldp` | 1900
  - Configuring LLDP
  - `show lldp neighbors`
power-negotiation

Syntax

```conf
case: power-negotiation {
  disable;
}
```

Hierarchy Level

```
[edit protocols lldp interface (all | interface-name)]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure Link Layer Discovery Protocol (LLDP) power negotiation, which negotiates with Power over Ethernet (PoE) powered devices to allocate power.

LLDP power negotiation requires the PoE management option to be set to class.

The remaining statement is explained separately. See CLI Explorer.

Default

LLDP power negotiation is enabled by default when the PoE management option is set to class.

Required Privilege Level

routing—To view this statement in the configuration.

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Related Documentation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring LLDP (CLI Procedure)</td>
<td>654</td>
</tr>
<tr>
<td>Configuring PoE on EX Series Switches (CLI Procedure)</td>
<td></td>
</tr>
</tbody>
</table>
preference (Subscriber Management)

Syntax

```
preference route-distance;
```

Hierarchy Level

```
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options access route prefix],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name access route prefix],
[edit dynamic-profiles profile-name routing-options access route prefix]
```

Release Information

Statement introduced in Junos OS Release 9.5.

Description

Dynamically configure the distance for an access route.

Options

route-distance—Either the specific distance you want to assign to the access route or either of the following distance variables:

- `$junos-framed-route-distance`—Distance of an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-Route attribute [22].
- `$junos-framed-route-ipv6-distance`—Distance of an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-IPv6-Route attribute [99].

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Dynamic Access Routes for Subscriber Management
preferred-prefix-length

Syntax

preferred-prefix-length preferred-prefix-length;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client prefix-delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]

Release Information
Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100. The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description
Allows you to configure DHCPv6 client preferred prefix length. If preferred-prefix-length is configured, the DHCPv6 client checks the prefix length in the ADVERTISE packet and if the check fails, a syslog is created.

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

RELATED DOCUMENTATION

sub-prefix-length  | 2299
prefix (DHCP Client)

Syntax

```plaintext
prefix {
  host-name;
  logical-system-name;
  routing-instance-name;
}
```

Hierarchy Level

```plaintext
[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-identifier]
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Specify a prefix as a client identifier.

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

RELATED DOCUMENTATION
prefix (DHCP Relay Agent)

Syntax

prefix prefix;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.

Description

Add a prefix to the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or to the DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID) information in DHCP packets that DHCP relay agent sends to a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.

Options

prefix—Any of the following:

- host-name—Prepend the hostname of the router configured with the host-name statement at the [edit system] hierarchy level to the DHCP option information.
- logical-system-name—Prepend the name of the logical system to the option information.
- routing-instance-name—Prepend the name of the routing instance to the option information.

Required Privilege Level

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

RELATED DOCUMENTATION

Including a Prefix in DHCP Options

Using DHCP Relay Agent Option 82 Information | 739

Configuring DHCPv6 Relay Agent Options
process-inform

Syntax

```process-inform {
    pool pool-name;
}
```

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name interface interface-name overrides],
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group group-name overrides],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server group group-name interface interface-name overrides]

**Release Information**
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**
Enable the processing of DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) sent from the client to request DHCP options. For DHCP local servers, the messages are also passed to the configured server list.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Default**
Information request messages are not processed.

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

**RELATED DOCUMENTATION**
- Enabling Processing of Client Information Requests | 839
- Overriding the Default DHCP Local Server Configuration Settings Overview | 807
profile (Access)

Syntax

```
profile profile-name {
    accounting {
        address-change-immediate-update
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        ancp-speed-change-immediate-update;
        coa-immediate-update;
        coa-no-override service-class-attribute;
        duplication;
        duplication-filter;
        duplication-vrf {
            access-profile-name profile-name;
            vrf-name vrf-name;
        }
        immediate-update;
        order [ accounting-method ];
        send-acct-status-on-config-change;
        statistics (time | volume-time);
        update-interval minutes;
        wait-for-acct-on-ack;
    }
    accounting-order (radius | [accounting-order-data-list]);
    authentication-order [ authentication-methods ];
    client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
            ike-policy policy-name;
            interface-id string-value;
        }
        l2tp {
            aaa-access-profile profile-name;
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
            maximum-sessions number;
        }
    }
```
maximum-sessions-per-tunnel number;
multilink {
    drop-timeout milliseconds;
    fragment-threshold bytes;
}
override-result-code session-out-of-resource;
ppp-authentication (chap | pap);
ppp-profile profile-name;
service-profile profile-name(parameter) & profile-name;
sessions-limit-group limit-group-name;
shared-secret shared-secret;
}

pap-password pap-password;

ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-ip-address ip-address;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}

user-group-profile profile-name;

}

domain-name-server;
domain-name-server-inet;
domain-name-server-inet6;
local {
    flat-file-profile profile-name;
}

preauthentication-order preauthentication-method;
provisioning-order (gx-plus | jsrc | pcrf);
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude {
            attribute-name packet-type;
            standard-attribute number {
                packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
            }
            vendor-id id-number {
                vendor-attribute vsa-number {
                    packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
                }
            }
        }
        ignore {
            dynamic-ifset-name;
            framed-ip-netmask;
            idle-timeout;
            input-filter;
            logical-system: routed-instance;
            output-filter;
            session-timeout;
            standard-attribute number;
            vendor-id id-number {
                vendor-attribute vsa-number;
            }
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            interface-text-description;
            mac-address;
            nas-identifier;
            stacked-vlan;
            vlan;
        }
        chap-challenge-in-request-authenticator;
        client-accounting-algorithm (direct | round-robin);
    }
}
client-authentication-algorithm (direct | round-robin);
coa-dynamic-variable-validation;
ethernet-port-type-virtual;
interface-description-format {
    exclude-adapter;
    exclude-channel;
    exclude-sub-interface;
}
juniper-access-line-attributes;
nas-identifier identifier-value;
nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    pw-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
        adapter-width width;
        port-width width;
        slot-width width;
        vci-width width;
        vpi-width width;
    }
}
nas-port-id-delimiter delimiter-character;
nas-port-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    interface-text-description;
    nas-identifier;
    order {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        interface-text-description;
        nas-identifier;
        postpend-vlan-tags;
    }
    postpend-vlan-tags;
}
nas-port-type {
    ethernet {
        port-type;
    }
}

override {
    calling-station-id remote-circuit-id;
    nas-ip-address tunnel-client-gateway-address;
    nas-port tunnel-client-nas-port;
    nas-port-type tunnel-client-nas-port-type;
}

remote-circuit-id-delimiter;

remote-circuit-id-fallback {
    remote-circuit-id-format;
    agent-circuit-id;
    agent-remote-id;
}

revert-interval interval;

service-activation {
    dynamic-profile (optional-at-login | required-at-login);
    extensible-service (optional-at-login | required-at-login);
}

vlan-nas-port-stacked-format;

preauthentication-server ip-address;

radius-server server-address {
    accounting-port port-number;
    accounting-retry number;
    accounting-timeout seconds;
    dynamic-request-port
    port port-number;
    preauthentication-port port-number;
    preauthentication-secret password;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    max-outstanding-requests value;
    source-address source-address;
    timeout seconds;
}
service {
  accounting {
    statistics (time | volume-time);
    update-interval minutes;
  }
  accounting-order (activation-protocol | local | radius);
}
session-limit-per-username number;
session-options {
  client-idle-timeout minutes;
  client-idle-timeout-ingress-only;
  client-session-timeoutminutes;
  pcc-context {
    input-service-filter-name filter-name;
    input-service-set-name service-set-name;
    ipv6-input-service-filter-name filter-name;
    ipv6-input-service-set-name service-set-name;
    ipv6-output-service-filter-name filter-name;
    ipv6-output-service-set-name service-set-name;
    output-service-filter-name filter-name;
    output-service-set-name service-set-name;
    profile-name pcef-profile-name;
  }
  strip-user-name {
    delimiter [ delimiter ];
    parse-direction (left-to-right | right-to-left);
  }
}
subscriber username {
  delegated-pool delegated-pool-name;
  framed-ip-address ipv4-address;
  framed-ipv6-pool ipv6-pool-name;
  framed-pool ipv4-pool-name;
  password password;
  target-logical-system logical-system-name <target-routing-instance (default | routing-instance-name)>;
  target-routing-instance (default | routing-instance-name);
}
}

Hierarchy Level

[edit access]
Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure a subscriber access profile that includes subscriber access, L2TP, or PPP properties.

Options

profile-name—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

Configuring the PPP Authentication Protocol
Configuring Access Profiles for L2TP or PPP Parameters
Configuring L2TP Properties for a Client-Specific Profile
Configuring an L2TP Access Profile on the LNS
Configuring an L2TP LNS with Inline Service Interfaces
Configuring PPP Properties for a Client-Specific Profile
Configuring Service Accounting with JSRC
Configuring Service Accounting in Local Flat Files
AAA Service Framework Overview
Enabling Direct PCC Rule Activation by a PCRF for Subscriber Management
**profile**

**Syntax**

```plaintext
profile profile-name {
    accounting {
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        order (radius [ [ accounting-order-data-list ];
    }
    authentication-order [authentication-method];
    radius {
        accounting-server [server-addresses];
        authentication-server [server-addresses];
    }
}
```

**Hierarchy Level**

```
[edit access]
```

**Release Information**

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

**Description**

Configure an access profile. The access profile contains the entire authentication, authorization, and accounting (AAA) configuration that aids in handling AAA requests, including the authentication method and order, AAA server addresses, and AAA accounting.

**Default**

Not enabled.

**Options**

`profile-name`—Profile name of up to 32 characters.

The remaining statements are explained separately. See CLI Explorer.

---

**NOTE:** The [edit access] hierarchy is not available on QFabric systems.
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438
profilerd

Syntax

```
profilerd {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the profiler process.

Options

- **command binary-file-path**—Path to binary for process.
- **disable**—Disable the profiler process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
- **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
- **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

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

**Syntax**

```plaintext
protocol-master (inet | inet6);
```

**Hierarchy Level**

```plaintext
[edit bridge-domains name forwarding-options dhcp-relay dhcpv6 group group-name dual-stack-group dual-stack-group-name],
[edit bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit logical-systems name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit logical-systems name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
```
[edit routing-instances name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit routing-instances name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit routing-instances name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name]

Release Information
Statement introduced in Junos OS Release 17.3.

Description
Select family as protocol master. In some customer use cases, CPE devices have reachability to multiple BNG routers for load sharing. The CPE's DHCP client broadcasts a DHCP protocol handshake to the reachable routers; more than one router may respond. In a DHCP dual-stack environment, the DHCPv4 and DHCPv6 protocol handshakes are independent of each other, meaning that each arm of the subscriber session could connect to a different router. You can avoid this situation by specify the master protocol. For a given dual-stack subscriber, this configuration causes the rejection of any binding attempt from the secondary address family client when a binding is not currently active for the master protocol family. If bindings are currently active for both arms when the master protocol family binding is released or deleted, then the binding for the secondary address family is also torn down.

Options
inet—INET family has protocol master behavior.
inet6—INET6 family has protocol master behavior.

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

- Configuring Access Profile Options for Interactions with RADIUS Servers
- Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
- Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution
- Configuring Access Components for the PPPoE Wholesale Network Solution
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
**protocol-version**

**Syntax**

```bash
protocol-version [v2];
```

**Hierarchy Level**

```bash
[edit system services ssh]
```

**Release Information**

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

**Description**

Specify the Secure Shell (SSH) protocol version.

Starting in Junos OS Release 19.3R1 and Junos OS Release 18.3R3, on all SRX Series devices, we’ve removed the nonsecure SSH protocol version 1 (v1) option from the `[edit system services ssh protocol-version]` hierarchy level. You can use the SSH protocol version 2 (v2) as the default option to remotely manage systems and applications. With the v1 option deprecated, Junos OS is compatible with OpenSSH 7.4 and later versions.

Junos OS Release earlier to 19.3R1 and 18.3R3 continue to support the v1 option to remotely manage systems and applications.

**Default**

v2—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

**Options**

SSH protocol version v2.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring SSH Service for Remote Access to the Router or Switch | 294
protocols

Syntax

protocols {
    bgp {
        disable;
        accept-remote-nexthop;
        advertise-external <conditional>;
        advertise-inactive;
        (advertise-peer-as | no-advertise-peer-as);
        authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
        authentication-key key;
        authentication-key-chain key-chain;
        bfd-liveness-detection {
            authentication {
                algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 | meticulous-keyed-sha-1 | simple-password);
                key-chain key-chain-name;
                loose-check;
            }
            detection-time {
                threshold milliseconds;
            }
            hold-down-interval milliseconds;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (1 | automatic);
        }
        cluster cluster-identifier;
        damping;
        description text-description;
        export [ policy-names ];
        family family-name {
            ... the family subhierarchies appear after the main [edit protocols bgp] hierarchy ...
        }
        graceful-restart {
            disable;
restart-time seconds;
stale-routes-time seconds;
}
group group-name {
    ... the group subhierarchy appears after the main [edit protocols bgp] hierarchy ...
}
hold-time seconds;
import [ policy-names ];
include-mp-next-hop;
keep (all | none);
local-address address;
local-as autonomous-system <loops number> <alias> <private>;
local-preference local-preference;
log-updown;
metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
mtu-discovery;
multihop {
    no-nexthop-change;
    ttl ttl-value;
}
no-aggregator-id;
no-client-reflect;
out-delay seconds;
outbound-route-filter {
    bgp-orf-cisco-mode;
prefix-based {
        accept {
            inet {
                inet;
                inet6;
            }
        }
    }
}
passive;
path-selection {
    always-compare-med;
    as-path-ignore;
    cisco-non-deterministic;
    external-router-id;
    med-plus-igp {
        igp-multiplier number;
        med-multiplier number;
    }
}
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>;
  flag <flag-modifier> <disable>;
}
dcbx {
disable;
interface (interface-name | all) {
disable;
  application-map application-map-name;
  applications {
    no-auto-negotiation;
  }
  enhanced-transmission-selection {
    no-auto-negotiation;
    no-recommendation-tlv;
    recommendation-tlv {
      no-auto-negotiation;
    }
  }
  dcbx-version (auto-negotiate | ieee-dcbx | dcbx-version-1.01);
  priority-flow-control {
    no-auto-negotiation;
  }
}
}
iccp {
    authentication-key string;
    local-ip-addr local-ip-addr;
    peer ip-address{
        authentication-key string;
        backup-liveness-detection {
            backup-peer-ip ip-address;
        }
        liveness-detection {
            detection-time {
                threshold milliseconds;
            }
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (Liveness Detection) (1 | automatic);
        }
        local-ip-addr ipv4-address;
        session-establishment-hold-time seconds;
    }
    session-establishment-hold-time seconds;
    traceoptions {
        file <filename> <files number> <match regular-expression> <microsecond-stamp> <size size> <world-readable |
        no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
igmp-snooping {
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
        flag flag (detail | disable | receive | send);
    }
    (vlan | vlan) vlan-name {
        disable;
        immediate-leave;
        (interface | interface) interface-name {
            group-limit limit;
            host-only-interface;
            immediate-leave;
            multicast-router-interface;
            (static | static){
                (group | group) multicast-ip-address {
                    source ip-address;
                }
            }
        }
        query-interval seconds;
        query-last-member-interval seconds;
        query-response-interval seconds;
        robust-count number;
    }
}
isis {
    disable;
    export [ policy-names ];
    ignore-attached-bit;
    interface interface-name {
        bfd-liveness-detection {
            authentication {
                algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 | meticulous-keyed-sha-1 | simple-password);
                key-chain key-chain-name;
                loose-check;
            }
            detection-time {
                threshold milliseconds;
            }
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (1 | automatic);
        }
        checksum;
        csnp-interval (seconds | disable);
        disable;
        hello-padding (adaptive | loose | strict);
        level (1 | 2) {
            disable;
            hello-authentication-key key;
            hello-authentication-type authentication;
            hello-interval seconds;
            hold-time seconds;
            ipv4-multicast-metric number;
            metric metric;
            passive;
            priority number;
        }
        lsp-interval milliseconds;
        mesh-group (value | blocked);
        no-ipv4-multicast;
        no-unicast-topology;
        passive;
point-to-point;
}
level (1 | 2) {
    disable;
    authentication-key key;
    authentication-type authentication;
    external-preference preference;
    no-csnp-authentication;
    no-hello-authentication;
    no-psnp-authentication;
    preference preference;
    prefix-export-limit number;
    wide-metrics-only;
}
loose-authentication-check;
lsp-lifetime seconds;
max-areas number;
no-adjacency-holdown;
no-authentication-check;
no-ipv4-routing;
overload {
    advertise-high-metrics;
    timeout seconds;
}
reference-bandwidth reference-bandwidth;
rib-group {
    inet group-name;
}
topologies {
    ipv4-multicast;
}
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
traffic-engineering {
    disable;
    family inet {
        shortcuts {
            multicast-rpf-routes:
        }
    }
}
}
lldp {
    disable;
    advertisement-interval seconds;
    hold-multiplier number;
    interface (LLDP) (all | interface-name) {
        disable;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
    flag flag (detail | disable | receive | send);
}
}
mstp {
    disable;
    bpdu-timeout-action;
    bridge-priority priority;
    configuration-name name;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        bpdu-timeout-action {
            block;
            alarm;
        }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    max-hops hops;
    msti msti-id {
        vlan (vlan-id | vlan-name);
        interface interface-name {
            disable;
            cost cost;
            edge;
            mode mode;
            priority priority;
        }
    }
    revision-level revision-level;
    traceoptions {
        file filename <files number > <size> <no-stamp | world-readable | no-world-readable>;
        flag flag;
    }
}
ospf {
    disable;
    area area-id {
        area-range ip-prefix/<prefix-length> <exact> <override-metric metric> <restrict>;
        context-identifier identifier
        interface interface-name {
            disable;
            authentication {
                md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
                simple-password key-string;
            }
            bandwidth-based-metrics {
                bandwidth value metric number;
            }
            bfd-liveness-detection {
                authentication {
                    algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 | meticulous-keyed-sha-1 | simple-password);
                    key-chain key-chain-name;
                    loose-check;
                }
                detection-time {
                    threshold milliseconds;
                }
                full-neighbors-only;
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
                version (1 | automatic);
            }
            dead-interval seconds;
            dynamic-neighbors;
            flood-reduction;
            hello-interval seconds;
            interface-type (nbma | p2mp | p2p);
            metric metric;
            neighbor address <eligible>;
            no-eligible-backup;
            no-interface-state-traps;
        }
    }
}
no-neighbor-down-notification;
passive {
    traffic-engineering {
        remote-node-id address;
    }
}
poll-interval seconds;
priority number;
retransmit-interval seconds;
secondary;
te-metric metric;
topology (name | default | ipv4-multicast) {
    disable;
    bandwidth-based-metrics {
        bandwidth value;
        metric number;
    }
    metric metric;
}
transit-delay seconds;
}

network-summary-export [ policy-names ];
network-summary-import [ policy-names ];
nssa {
    area-range ip-prefix prefix-length exact override-metric metric restrict;
    default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
    }
    (summaries | no-summaries);
}
stub <default-metric metric> <summaries | no-summaries>;
virtual-link neighbor-id router-id transit-area area-id {
  disable;
  authentication {
    md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
    simple-password key-string;
  }
  dead-interval seconds;
  demand-circuit;
  flood-reduction;
  hello-interval seconds;
  ipsec-sa sa-name;
  no-neighbor-down-notification;
  retransmit-interval seconds;
  topology (name | default | ipv4-multicast) {
    disable;
    metric metric;
  }
  transit-delay seconds;
}

database-protection {
  ignore-count number;
  ignore-time seconds;
  maximum-lsa number;
  reset-time seconds;
  warning-only;
  warning-threshold percent;
}
export [ policy-names ];
external-preference preference;
graceful-restart {
  disable;
  helper-disable <both | restart-signaling | standard>;
  no-strict-lsa-checking;
  notify-duration seconds;
  restart-duration seconds;
}
import [ policy-names ];
no-nssa-abr;
no-rfc-1583;
overload <timeout seconds>;
preference preference;
prefix-export-limit number;
reference-bandwidth reference-bandwidth;
rib-group group-name;
topology (default | ipv4-multicast | name) {
    overload;
    prefix-export-limit number;
    topology-id number;
}
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
traffic-engineering {
    advertise-unnumbered-interfaces;
    credibility-protocol-preference;
    ignore-lsp-metrics;
    multicast-rpf-routes;
    no-topology;
    shortcuts <lsp-metric-into-summary>;
}
pim {
    disable;
    assert-timeout seconds;
    dense-groups {
        addresses;
    }
    dr-election-on-p2p;
    export;
    family (inet | inet6) {
        disable;
    }
    graceful-restart {
        disable;
        restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
        accept-remote-source;
        disable;
        family (inet | inet6) {
            disable;
        }
        hello-interval seconds;
        mode (dense | sparse | sparse-dense);
        neighbor-policy [ policy-names ];
        override-interval milliseconds;
        priority number;
        propagation-delay milliseconds;
        reset-tracking-bit;
        version version;
    }
    join-load-balance;
    join-prune-timeout;
    nonstop-routing;
    override-interval milliseconds;
    propagation-delay milliseconds;
    reset-tracking-bit;
    rib-group group-name;
    rp {
        auto-rp {
            (announce | discovery | mapping);
            (mapping-agent-election | no-mapping-agent-election);
        }
    }
    bootstrap {
family (inet | inet6) {
    export [ policy-names ];
    import [ policy-names ];
    priority number;
}
bootstrap-import [ policy-names ];
bootstrap-export [ policy-names ];
bootstrap-priority number;
dr-register-policy [ policy-names ];
embedded-rp {
    group-ranges {
        destination-ip-prefix</prefix-length>;
    }
    maximum-rps limit;
}
local {
    family (inet | inet6) {
        address address;
        anycast-pim {
            disable;
            rp-set {
                address address <forward-msdp-sa>;
            }
            local-address address;
        }
        group-ranges {
            destination-ip-prefix</prefix-length>;
        }
    }
    hold-time seconds;
    priority number;
}
rp-register-policy [ policy-names ];
spt-threshold {
    infinity [ policy-names ];
}
static {
    address address {
        group-ranges {
            version version;
            destination-ip-prefix</prefix-length>;
        }
    }
}
}
}
rpf-selection {
    group group-address{
        source source-address{
            next-hop next-hop-address;
        }
        wildcard-source {
            next-hop next-hop-address;
        }
    }
    prefix-list prefix-list-addresses {
        source source-address {
            next-hop next-hop-address;
        }
        wildcard-source {
            next-hop next-hop-address;
        }
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
tunnel-devices [ mt-fpc/pic/port ];
}
rip {
  authentication-key password;
  authentication-type type;
  (check-zero | no-check-zero);
  group group-name {
    bfd-liveness-detection {
      authentication {
        algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 | meticulous-keyed-sha-1 | simple-password);
        key-chain key-chain-name;
        loose-check;
      }
      detection-time {
        threshold milliseconds;
      }
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    export [ policy-names ];
    import [ policy-names ];
  }
  metric-out metric;
  neighbor neighbor-name {
    any-sender;
    authentication-key password;
    authentication-type type;
    bfd-liveness-detection {
      ... same statements as at the [edit protocols rip group group-name bfd-liveness-detection] hierarchy level ...
    }
    (check-zero | no-check-zero);
    import [ policy-names ];
    message-size number;
    metric-in metric;
    receive (both | none | version-1 | version-2);
    route-timeout seconds;
    send (broadcast | multicast | none | version-1);
    update-interval seconds;
  }
}
preference preference;
route-timeout seconds;
update-interval seconds;
}
holddown seconds;
import [ policy-names ];
message-size number;
metric-in metric;
receive (both | none | version-1 | version-2);
rib-group group-name;
route-timeout seconds;
send (broadcast | multicast | none | version-1);
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
update-interval seconds;
}
ratp {
  disable;
bpdu-block-on-edge;
bridge-priority priority;
forward-delay seconds;
hello-time seconds;
interface (all | interface-name) {
  disable;
bpdu-timeout-action {
    alarm;
    block;
  }
cost cost;
edge;
mode mode;
no-root-port;
priority priority;
}
max-age seconds;
}
traceoptions {
  file filename <files number> <size> <no-stamp> <world-readable | no-world-readable>;
  flag flag;
}
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        bpdu-timeout-action {
            alarm;
            block;
        }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
}
traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>;
    flag flag;
}
uplink-failure-detection {
    group group-name {
        link-to-monitor interface-name;
        link-to-disable interface-name;
    }
}
Hierarchy Level

[edit]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure protocols.

The remaining statements are explained separately. See CLI Explorer.
Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Junos OS Routing Protocols Configuration Guide
provisioning-order (Diameter Applications)

**Syntax**

```
provisioning-order (gx-plus | jsrc | pcrf);
```

**Hierarchy Level**

```
[edit access profile profile-name]
```

**Release Information**

Support for Gx-Plus introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
pjcr option added in Junos OS Release 16.2.

**Description**

Configure AAA to use the specified application for subscriber service provisioning.

**Options**

- `gx-plus`—Specify Gx-Plus as the application used to communicate with a PCRF server for subscriber service provisioning. Sets the Subscription-Id-Type Diameter AVP sub-attribute (450) to 4 (END_USER_PRIVATE) and sets the Subscription-Id-Data Diameter AVP sub-attribute (444) to `reserved`. Both of these sub-attributes are conveyed in the Diameter AVP Subscription-ID (443) by a CCR-I message.

- `jsrc`—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.

- `pcrf`—Specify Policy Control and Charging Rules Function (PCRF) as the application used to request provisioning from the PCRF server over the Gx protocol. If you change this configuration, any existing subscriber sessions are unaffected.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *JSRC Configuration Overview*
<table>
<thead>
<tr>
<th>Provisioning Subscribers with JSRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Gx-Plus</td>
</tr>
<tr>
<td><strong>Provisioning Subscribers with Gx-Plus</strong></td>
</tr>
<tr>
<td>Understanding Gx Interactions Between the Router and the PCRF</td>
</tr>
<tr>
<td>Understanding Interactions Between the PCRF, PCEF, and OCS</td>
</tr>
</tbody>
</table>
proxy

Syntax

proxy {
    password password;
    port port-number;
    server url;
    username user-name;
}

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the proxy information for the router.

Options

- **password password**—Password configured in the proxy server.
- **port port number**—Proxy server port number.
  
    Range: 0 through 65,535
- **server url**—URL or IP address of the proxy server host.
- **username username**—Username configured in the proxy server.

Required Privilege Level

system—To view this statement in the configuration.

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

Syntax

proxy-mode;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface overrides],

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.

You cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.

Required Privilege Level

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>DHCP Relay Proxy Overview</th>
<th>826</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>Enabling DHCP Relay Proxy Mode</td>
<td>828</td>
</tr>
</tbody>
</table>
ptopo-configuration-maximum-hold-time

Syntax

```
ptopo-configuration-maximum-hold-time seconds;
```

Hierarchy Level

```
[edit protocols lldp],
[edit routing-instances routing-instance-name protocols lldp]
```

Release Information

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

Description

Configure how long to maintain the physical topology database entries. The physical topology identifies the devices on the network and their physical interconnections.

Options

- `seconds`—Time to maintain physical topology entries.

Default: 300

Range: 1 through 2147483647

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring LLDP
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
- Understanding LLDP | 653
ptopo-configuration-trap-interval

Syntax

ptopo-configuration-trap-interval seconds;

Hierarchy Level

[edit protocols lldp],
[edit routing-instances routing-instance-name protocols lldp]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify how often SNMP trap notifications are sent to the Master Agent regarding changes in physical
 topology global statistics.

Options
seconds—Specify how often SNMP trap notifications are sent. This feature is disabled by default.

Range: 0 through 3600

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

RELATED DOCUMENTATION

Configuring LLDP
push-backup-to-master (Accounting Options)

Syntax

```
push-backup-to-master;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information


Description

Configure the router to save the accounting files from the new backup Routing Engine to the new master Routing Engine when a change in mastership occurs. The files are saved to the `/var/log/pfedBackup` directory on the router. The master Routing Engine includes these accounting files with its own current accounting files when it transfers the files from the backup directory to the archive site at the next transfer interval. Use this statement when the new backup Routing Engine is not able to connect to the archive site; for example, when site is not connected by means of an out-of-band interface or the path to the site is routed through a line card.

NOTE: The backup Routing Engine's files on the master Routing Engine are sent at each interval even though the files remain the same. If this is more activity than you want, consider using the `backup-on-failure master-and-slave` statement instead.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Accounting-Data Log Files
- Configuring Flat-File Accounting for Layer 2 Wholesale
- Configuring Flat-File Accounting for Extensible Subscriber Services Management
- Flat-File Accounting Overview
quiet-period

Syntax

quiet-period seconds;

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names])]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.3 for MX Series and SRX Series.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

For 802.1X authentication, configure the number of seconds the interface remains in the wait state following a failed authentication attempt by a supplicant before reattempting authentication.

Default

60 seconds

Options

seconds—Number of seconds the interface remains in the wait state.

Range: 0 through 65,535 seconds
Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

show network-access aaa statistics authentication | 2714
Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
quiet-period (Captive Portal)

**Syntax**

```yaml
quiet-period seconds;
```

**Hierarchy Level**

```bash
[edit services captive-portal interface (all | interface-names)]
```

**Release Information**

Statement introduced in Junos OS Release 10.1 for EX Series switches.

**Description**

Configure time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.

**Options**

- `seconds`—Number of seconds.

**Range:** 1–65535

**Default:** 60

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492
radius

Syntax

radius {
   accounting-server [server-addresses];
   authentication-server [server-addresses];
}

Hierarchy Level

[edit access profile profile-name]

Release Information

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

Description

Configure the RADIUS servers for authentication and for accounting. To configure multiple RADIUS servers, include multiple radius statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The [edit access] hierarchy is not available on QFabric systems.

Required Privilege Level

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

RELATED DOCUMENTATION

| Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400 |
| Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438 |
| Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395 |
radius (Access Profile)

Syntax

radius {
  accounting-server [ ip-address ];
  attributes {
    exclude
      attribute-name packet-type;
    standard-attribute number {
      packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
    }
    vendor-id id-number {
      vendor-attribute vsa-number {
        packet-type [ access-request | accounting-off | accounting-on | accounting-start | accounting-stop ];
      }
    }
  }
  ignore {
    dynamic-iflset-name;
    framed-ip-netmask;
    idle-timeout;
    input-filter;
    logical-system-routing-instance;
    output-filter;
    session-timeout;
    standard-attribute number;
    vendor-id id-number {
      vendor-attribute vsa-number;
    }
  }
  authentication-server [ ip-address ];
  options {
    accounting-session-id-format (decimal | description);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      nas-identifier;
    }
    chap-challenge-in-request-authenticator;
    client-accounting-algorithm (direct | round-robin);
client-authentication-algorithm (direct | round-robin);
coa-dynamic-variable-validation;
ethernet-port-type-virtual;
interface-description-format {
  exclude-adapted;
  exclude-channel;
  exclude-sub-interface;
}
ip-address-change-notify message;
juniper-access-line-attributes;
nas-identifier identifier-value;
nas-port-extended-format {
  adapter-width width;
  ae-width width;
  port-width width;
  slot-width width;
  stacked-vlan-width width;
  vlan-width width;
  atm {
    adapter-width width;
    port-width width;
    slot-width width;
    vci-width width;
    vpi-width width;
  }
}
nas-port-id-delimiter delimiter-character;
nas-port-id-format {
  agent-circuit-id;
  agent-remote-id;
  interface-description;
  interface-text-description;
  nas-identifier;
  order {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    interface-text-description;
    nas-identifier;
    postpend-vlan-tags;
  }
  postpend-vlan-tags;
}
nas-port-type {
    ethernet {
        port-type;
    }
}
override {
    calling-station-id remote-circuit-id;
    nas-ip-address tunnel-client-gateway-address;
    nas-port tunnel-client-nas-port;
    nas-port-type tunnel-client-nas-port-type;
}
remote-circuit-id-delimiter;
remote-circuit-id-fallback;
remote-circuit-id-format {
    agent-circuit-id;
    agent-remote-id;
}
revert-interval interval;
service-activation {
    dynamic-profile (optional-at-login | required-at-login);
    extensible-service (optional-at-login | required-at-login);
}
vlan-nas-port-stacked-format;
preauthentication-server ip-address;

Hierarchy Level

[edit access profile profile-name]

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

Description
Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.
Options

**accounting-server**—(MX Series only) Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

Values: *ip-address*—IP version 4 (IPv4) address.

**authentication-server**—(SRX Series only) Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Values: *ip-address*—IPv4 address.

**preauthentication-server**—(MX Series only) Starting in Junos OS Release 13.3, specify the RADIUS preauthentication server, which is used for the LLID service.

NOTE: You cannot configure this statement if the Calling-Station-ID attribute is excluded from RADIUS Access-Request messages by the *exclude* statement.

Values: *ip-address*—IPv4 address.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

admin—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- [Configuring Authentication and Accounting Parameters for Subscriber Access](#)
- [RADIUS Logical Line Identifier (LLID) Overview](#)
- [Configuring Logical Line Identification (LLID) Preauthentication](#)
radius (System)

Syntax

radius {
    server {
        server-address {
            accounting-port port-number;
            secret password;
            source-address address;
            retry number;
            timeout seconds;
        }
    }
}

Hierarchy Level

[edit system accounting destination]

Release Information
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure the RADIUS accounting server.

Options
server-address—Address of the RADIUS accounting server.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring RADIUS System Accounting | 255
radius-disconnect (DHCP Local Server)

Syntax

radius-disconnect;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure trigger],
[edit system services dhcp-local-server reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit system services dhcp-local-server group group-name reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure trigger]

Release Information
Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description
Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.

Default
The client is deleted when a RADIUS-initiated disconnect is received.

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

**RELATED DOCUMENTATION**

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | 848
radius-options

Syntax

radius-options {
   attributes {
      nas-ip-address nas-ip-address;
   }
   password-protocol mschap-v2;
}

Hierarchy Level

[edit system]

Release Information
Statement introduced in Junos OS Release 8.5. Support for network access server (NAS) IPv6 address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description
Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options
• attributes—Configure RADIUS attributes.
  • nas-ip-address nas-ip-address—Valid IPv4 or IPv6 address of the NAS requesting user authentication.
• password-protocol mschap-v2—Protocol MS-CHAPv2, used for password authentication and password changing.

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

RELATED DOCUMENTATION
radius-server | 2154
radius-options (802.1X)

Syntax

```plaintext
radius-options {
  use-vlan-id;
  use-vlan-name;
}
```

Hierarchy Level

```plaintext
[edit protocols dot1x authenticator]
```

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure 802.1X authenticator so that the VLAN ID or VLAN name is included in the packet sent to the RADIUS server to request authentication.

Options

- **use-vlan-id**—Include the VLAN ID in the packet sent to the RADIUS server to request authentication.
- **use-vlan-name**—Include the VLAN name in the packet sent to the RADIUS server to request authentication. The VLAN name is sent even if the 802.1X interface is configured with the VLAN ID.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Specifying RADIUS Server Connections on Switches (CLI Procedure) | 379
- authenticator | 1510
radius-options (Access)

Syntax

radius-options {
    revert-interval seconds;
}

Hierarchy Level

[edit access];
[edit access profile profile-name]

Release Information
Statement introduced in Release 8.5 of Junos OS.

Description
Configure RADIUS options.

Options
The remaining statement is explained separately.

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

RELATED DOCUMENTATION

Junos OS Security Configuration Guide
radius-options (System)

Syntax

radius-options {
    attributes {
        nas-ip-address ip-address;
    }
    enhanced-accounting;
    password-protocol mschap-v2;
}

Hierarchy Level

[edit system]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

NOTE: The radius-options statement is not available on QFabric systems.


Description
Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options
enhanced-accounting—View the attribute values of a logged in user.
nas-ip-address ip-address—IP address of the network access server (NAS) that requests user authentication.
password-protocol mschap-v2—Protocol MS-CHAPv2, used for password authentication and password changing.

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

RELATED DOCUMENTATION

- Configuring MS-CHAPv2 for Password-Change Support | 381
- Configuring RADIUS System Accounting | 255
- enhanced-accounting | 1756
radius-server

Syntax

```
radius-server server-address {
    accounting-port port-number;
    port number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level

[edit system]

Release Information

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

Description

Configure a RADIUS server for Point-to-Point Protocol (PPP).

To configure multiple RADIUS servers, include multiple `radius-server` statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

`server-address`—Address of the RADIUS authentication server.

The remaining statements are explained separately. See CLI Explorer.

**NOTE:** The `accounting-port` and `source-address` options are not available on QFabric systems.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>RELATED DOCUMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring RADIUS Authentication (QFX Series or OCX Series)</strong></td>
</tr>
<tr>
<td>accounting-port</td>
</tr>
<tr>
<td>port</td>
</tr>
<tr>
<td>retry</td>
</tr>
<tr>
<td>secret</td>
</tr>
<tr>
<td>source-address</td>
</tr>
<tr>
<td>timeout</td>
</tr>
</tbody>
</table>
radius-server

Syntax

radius-server server-address {
    accounting-port port-number;
    accounting-retry number;
    accounting-timeout seconds;
    dynamic-request-port port-number;
    max-outstanding-requests value;
    port port-number;
    preauthentication-port port-number;
    preauthentication-secret password;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
}

Hierarchy Level

[edit access],
[edit access profile profile-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
max-outstanding-requests introduced in Junos OS Release 11.4.
dynamic-request-port option added in Junos OS Release 14.2R1 for MX Series routers.
preauthentication-port and preauthentication-secret options added in Junos OS Release 15.1 for MX Series routers.
accounting-port introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS). It was introduced in Junos OS without ELS in the following releases: Junos OS Releases 12.3R10, 14.1X53-D25, and 15.1R4 for EX Series switches.
Support for IPv6 server-address introduced in Junos OS Release 16.1.

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.
To configure multiple RADIUS servers, include multiple `radius-server` statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.
Options

server-address—IPv4 or IPv6 address of the RADIUS server.

accounting-port—(EX Series, M Series, MX Series, PTX Series, T Series only) Configure the port number on which to contact the RADIUS accounting server. This statement was introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS). It was introduced in Junos OS without ELS in the following releases: Junos OS Releases 12.3R10, 14.1X53-D25, and 15.1R4 for EX Series switches.

NOTE: Specifying the accounting port is optional, and port 1813 is the default. However, we recommend that you configure it in order to avoid confusion, as some RADIUS servers might refer to an older default.

Values: port-number—Port number on which to contact the RADIUS accounting server. Most RADIUS servers use port 1813, as specified in RFC 2866.

Default: 1813

accounting-retry—(MX Series, T Series only) Starting in Junos OS Release 14.1, configure the number of times the device retransmits RADIUS accounting messages when no response is received from the server. When you do not configure this statement, the number of retry attempts is determined by the retry statement.

NOTE: To successfully set a retry limit for the accounting servers different from the authentication servers, you must configure both the accounting-retry and accounting-timeout statements. If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the retry and timeout statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: number—Number of retry attempts.

Range: 0 through 100

Default: 0 (disabled)

accounting-timeout—(MX Series, T Series only) Starting in Junos OS Release 14.1, configure how long the local device waits to receive a response from a RADIUS accounting server before retransmitting the message. When you do not configure this statement, the length of the timeout is determined by the timeout statement.
NOTE: To successfully set a timeout value for the accounting servers different from the authentication servers, you must configure both the `accounting-retry` and `accounting-timeout` statements. If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the `retry` and `timeout` statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: 
- **seconds**—Duration of timeout period.
  - **Range:** 0 through 1000 seconds
  - **Default:** 0 (disabled)

**dynamic-request-port**—(MX Series only) Starting in Junos OS Release 14.2R1, specify the port that the router monitors for dynamic (CoA) requests from the specified RADIUS servers. You can configure a port globally or for a specific access profile.

You must either use the default port for all RADIUS servers or configure the same nondefault port for all RADIUS servers. This rule applies at both the global access and access profile levels.

NOTE: Any other configuration results in a commit check failure. Multiple port numbers—that is, different port numbers for different servers—are not supported.

Values: 
- **port-number**—Number of the monitored port.
  - **Default:** 3799 (as specified in RFC 5176)

**max-outstanding-requests**—(MX Series only) Starting in Junos OS Release 11.4, configure the maximum number of outstanding requests for this RADIUS server. An increase in this value is immediate while a decrease is more gradual if the current number of outstanding requests exceeds the new value.

Values: 
- **requests**—Maximum number of outstanding requests for this RADIUS server.
  - **Range:** 0 through 2000 outstanding requests per server
  - **Default:** 1000 outstanding requests per server

**port**—(EX Series, M Series, MX Series, SRX Series, T Series only) Configure the port number on which to contact the RADIUS server.

Values: 
- **port-number**—Port number on which to contact the RADIUS server.
  - **Default:** 1812 (as specified in RFC 2865)
preauthentication-port—(MX Series only) Starting in Junos OS Release 15.1 for MX Series routers, configure the port number on which to contact the RADIUS server for logical line identification (LLID) preauthentication requests. If you do not configure a separate UDP port for preauthentication purposes, the same UDP port that you configure for authentication messages by including the `port port-number` statement is used.

Values: `port-number`—Port number used for preauthentication requests to contact the RADIUS server.

preauthentication-secret—(MX Series only) Starting in Junos OS Release 15.1 for MX Series routers, configure the password to use with the RADIUS server for LLID preauthentication requests. If you do not configure a separate UDP password for preauthentication purposes, the same password that you configure for authentication messages by including the `secret password` statement is used. The secret password used by the local router must match the one used by the server.

Values: `password`—Password to use. To include spaces enclose the character string in quotation marks.

retry—(EX Series, M Series, MX Series, PTX Series, T Series only) Specify the number of times that the device is allowed to attempt to contact a RADIUS authentication or accounting server. You can override the retry limit for accounting servers with the `accounting-retry` statement.

NOTE: To successfully set a retry limit for the accounting servers different from the authentication servers, you must configure both the `accounting-retry` and `accounting-timeout` statements. If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the `retry` and `timeout` statements.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

Values: `attempts`—Number of times that the router is allowed to attempt to contact a RADIUS server.

Range: 1 through 100

Default: 3

routing-instance—(SRX Series, vSRX only) Configure the routing instance used to send RADIUS packets to the RADIUS server.

Values: `routing-instance-name`—Routing instance name.

source-address—(SRX Series, vSRX only) Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. Support for IPv6 `source-address` was introduced in Junos OS Release 16.1.

Values: `source-address`—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.
timeout—(SRX Series, vSRX only) Configure the amount of time that the local device waits to receive a response from RADIUS authentication and accounting servers. You can override the timeout value for accounting servers with the `accounting-timeout` statement.

**NOTE:** To successfully set a timeout value for the accounting servers different from the authentication servers, you must configure both the `accounting-retry` and `accounting-timeout` statements. If you configure only one of these statements, then the value you configure is ignored in favor of the values configured with the `retry` and `timeout` statements.

**NOTE:** The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

**Values:** seconds—Amount of time to wait.
- **Range:** 1 through 1000 seconds
- **Default:** 3 seconds

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring the PPP Authentication Protocol
- Configuring RADIUS Authentication for L2TP
- Configuring RADIUS System Accounting
- Configuring RADIUS-Initiated Dynamic Request Support
- RADIUS Logical Line Identifier (LLID) Overview
- RADIUS Attributes for LLID Preauthentication Requests
- `show network-access aaa statistics`
- `clear network-access aaa statistics`
radius-server

Syntax

```
radius-server server-address {
    accounting-port port-number;
    max-outstanding-requests value;
    port port-number;
    retry value;
    secret password;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced in Junos OS Release 8.5. Support for IPv6 source address added in Junos OS Release 12.1X47-D15 for SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Description

Configure RADIUS server address for subscriber access management, Layer 2 Tunnelling Protocol (L2TP), or (Point-to-Point Protocol (PPP).

To configure multiple RADIUS servers, include multiple `radius-server` statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

- `server-address`—Address of the RADIUS server.
- `accounting-port port-number`—RADIUS server accounting port number.
  
  Range: 1 through 65,335 files
  
  Default: 1813
- `port port-number`—RADIUS server authentication port number.
  
  Range: 1 through 65,335 files
  
  Default: 1812
- `retry value`—Number of times that the router is allowed to attempt to contact a RADIUS server.
• **secret password**—Password to use; it can include spaces if the character string is enclosed in quotation marks.

• **max-outstanding-requests** *value*—Maximum number of outstanding requests in flight to server.
  
  **Range:** 1 through 65,335 files

• **source-address** *source-address*—Valid IPv4 or IPv6 address configured on one of the router or switch interfaces.

• **timeout** *seconds*—Amount of time to wait.
  
  **Range:** 1 through 90 seconds

  **Default:** 3 seconds

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
radius-server (System)

Syntax

```plaintext
radius-server {
  server-address {
    accounting-port port-number;
    port number;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-address source-address;
    timeout seconds;
  }
}
```

Hierarchy Level

```
[edit system]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure a RADIUS server for Point-to-Point Protocol (PPP).

To configure multiple RADIUS servers, include multiple `radius-server` statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

- `server-address`—Address of the RADIUS authentication server.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
radsec

Syntax

```
radsec {
    destination id-number {
        address ip-address;
        max-tx-buffers number;
        id-reuse-timeout seconds;
        port port-number;
        source-address ip-address;
        tls-certificate certificate-name;
        tls-force-ciphers [medium | low];
        tls-min-version [v1.1 | v1.2];
        tls-peer-name x0.radsec.com;
        tls-timeout seconds;
    }
}
```

Hierarchy Level

[edit access]

Release Information

Statement introduced in Junos OS Release 19.1R1.

Description

Configure RADIUS over TLS, also known as RADSEC, to redirect regular RADIUS traffic to remote RADIUS servers connected over TLS. The TLS connection provides encryption, authentication, and data integrity for the exchange of RADIUS messages.

TLS relies on certificates and private-public key exchange pairs to secure the transmission of data between the RADSEC client and server. The RADSEC destination uses local certificates that are dynamically acquired from the Junos PKI infrastructure.

To enable RADSEC, you must specify the name of the local certificate. If a certificate is not available, or if the certificate was revoked, the RADSEC destination attempts to retrieve it every 300 seconds.

Default

RADSEC is not enabled by default.

Options

```
source-address ip-address — Source IP address of the dynamic request.
```
**id-reuse-timeout seconds**—Response timeout after which the RADIUS ID field value can be reused.

**Default:** 120 seconds

**port port-number**—(Optional) Port number of the RADSEC server.

**Default:** 2083

**source-port port-number**—(Optional) Source port to include in RADIUS messages.

**tls-certificate**—Provide the name of the local certificate.

**tls-force-ciphers [low | medium]**—(Optional) Allow lower-grade ciphers than the default.

**tls-min-version [v1.1 | v1.2]**—(Optional) Configure TLS version to limit the lowest supported versions of TLS that are enabled for SSL connections.

**Default:** v1.2

**tls-peer-name name**—Certified name of the RADSEC server.

**tls-timeout seconds**—Timeout for TLS negotiation.

**Default:** 5 seconds

**Required Privilege Level**

admin—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- RADIUS over TLS (RADSEC) | 259
radsec-destination

Syntax

radsec-destination id-number;

Hierarchy Level

[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]

Release Information
Statement introduced in Junos OS Release 19.1R1 for EX Series switches.

Description
Configure a RADIUS over TLS (RADSEC) server as the destination for RADIUS traffic. The RADIUS traffic is redirected from the RADIUS server to the RADSEC destination. You can redirect more than one RADIUS server to the same RADSEC destination.

Options
id-number—The unique ID number for the RADSEC destination.

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

RELATED DOCUMENTATION

RADIUS over TLS (RADSEC) | 259
**rapid-commit (DHCPv6 Client)**

**Syntax**

```plaintext
rapid-commit;
```

**Hierarchy Level**

```plaintext
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
```

**Release Information**

Statement introduced in Junos OS Release 12.1X45-D10.
The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

**Description**

Used to signal the use of the two-message exchange for address assignment.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- DHCPv6 Client Overview | 998
- Understanding DHCPv6 Client and Server Identification | 1005
# rapid-commit (DHCPv6 Local Server)

## Syntax

```
rapid-commit;
```

## Hierarchy Level

- `[edit system services dhcp-local-server dhcpv6 overrides]`
- `[edit system services dhcp-local-server dhcpv6 group group-name overrides]`
- `[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...]`
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 ...]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...]`

## Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

## Description

Configure DHCPv6 local server to recognize the Rapid Commit option (DHCPv6 option 14) in DHCPv6 solicit messages sent from the DHCPv6 client. When rapid commit is enabled for both DHCPv6 local server and the DHCPv6 client, a two-message handshake is used instead of the standard four-message handshake. You can enable rapid commit support on DHCPv6 local server globally, for a named group, or for a specific interface.

## Default

Rapid commit support is not enabled.

## Required Privilege Level

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

## RELATED DOCUMENTATION

- **Configuring DHCPv6 Rapid Commit (MX, EX)** | 790
- **Overriding the Default DHCP Local Server Configuration Settings Overview** | 807
rate-limit

Syntax

```plaintext
rate-limit limit;
```

Hierarchy Level

```plaintext
[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services tftp-server],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]
```

Release Information

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

Description

Configure the maximum number of connection attempts per minute, per protocol (either IPv6 or IPv4) on an access service. For example, a rate limit of 10 allows 10 IPv6 telnet session connection attempts per minute and 10 IPv4 telnet session connection attempts per minute.

Default

150 connections

Options

- **rate-limit limit**—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

  Range: 1 through 250

Default: 150

Required Privilege Level

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

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
reauthenticate (DHCP Local Server)

Syntax

```
reauthenticate (<lease-renewal> <remote-id-mismatch>);
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server],
[edit logical-systems name routing-instances name system services dhcp-local-server dhcpv6],
[edit logical-systems name system services dhcp-local-server],
[edit logical-systems name system services dhcp-local-server dhcpv6],
[edit logical-systems name system services dhcp-local-server dual-stack-group name],
[edit routing-instances name system services dhcp-local-server dhcpv6],
[edit routing-instances name system services dhcp-local-server dual-stack-group name],
[edit routing-instances name system services dhcp-local-server],
[edit routing-instances name system services dhcp-local-server dhcpv6],
[edit routing-instances name system services dhcp-local-server dual-stack-group name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dual-stack-group name]
```

Release Information

Statement introduced in Junos OS Release 17.4R1 on MX Series routers. Support at the `[edit ... system services dhcp-local-server dual-stack-group]` hierarchy level introduced in Junos OS Release 18.1R1.

Description

Enable DHCP client reauthentication, that is, trigger `jdhcpd` to request reauthentication from authd, which in turn reissues the RADIUS Access-Request for subscriber authentication. The purpose of the reauthentication is to change characteristics of the subscriber session, such as activating subscriber services or changing attributes. You can use reauthentication as an alternative to a RADIUS CoA request.

Starting in Junos OS Release 18.1R1, reauthentication can be triggered by discover and solicit messages in addition to the previously supported renew and rebinding messages. The release also introduces reauthentication support for dual-stack, single-session subscribers.

You can specify that reauthentication occurs in response to all DHCP renew, rebinding, discover, or solicit messages or only in response to discover and solicit messages that include a new (different) Agent Remote ID for the DHCP client.
You can use the Juniper Networks VSA, Reauthentication-On-Renew (26-206) as an alternative to the CLI configuration to enable reauthentication. The `reauthenticate` statement overrides the VSA when the VSA is present with a value of disable.

**NOTE:** Reauthentication for dual-stack, single-session subscribers requires that the `on-demand-address-allocation` statement is configured for the dual-stack group. This is true whether you enable reauthentication with the `reauthenticate` statement or the Reauthenticate-On-Renew VSA (26-206).

**NOTE:** You cannot configure both the `reauthenticate` statement and the `remote-id-mismatch` statement at the global level, `[edit system services dhcp-local-server]`. However, DHCP precedence rules do permit you to configure both statements when they are at different levels. For example, you can configure `reauthenticate` at the global level and `remote-id-mismatch` for DHCPv6 at the `[edit system services dhcp-local-server dhcpv6]` or for a specific group at the `[edit system services dhcp-local-server group name]` hierarchy level, and so on.

**NOTE:** Reauthentication does not support Extensible Services Subscriber Management (essmd) services. Activation or deactivation of any such service causes the request to fail.

**Options**

`lease-renewal`—Reauthenticate when a renew, rebind, discover, or solicit message is received from the DHCP client.

`remote-id-mismatch`—Reauthenticate when a discover or solicit message is received from the DHCP client with a new value for the DHCP client’s Agent Remote ID. The change in value corresponds to a change in subscriber service plan. The Agent Remote ID is conveyed in option 82, suboption 2 for DHCPv4 clients and in option 37 for DHCPv6 clients.

**Required Privilege Level**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.
RELATED DOCUMENTATION

Configuring RADIUS Reauthentication for DHCP Subscribers

RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers
reauthentication

Syntax

reauthentication interval;

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names])]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

The reauthentication statement is used to locally configure the number of seconds before the 802.1X authentication session times out and the client must reattempt authentication.

NOTE: If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the reauthentication statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

Options

interval—Sets the periodic reauthentication time interval in seconds.

Range: 1 through 4,294,967,296 seconds

Default: 3600 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring 802.1X Interface Settings (CLI Procedure) | 390
reconfigure (DHCP Local Server)

Syntax

reconfigure {
   attempts attempt-count;
   clear-on-abort;
   strict;
   support-option-pd-exclude;
   timeout timeout-value;
   token token-value;
   trigger {
      radius-disconnect;
   }
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name]

Release Information

Statement introduced in Junos OS Release 10.0.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
support-option-pd-exclude statement introduced in Junos OS Release 17.3 for the MX Series.
**Description**
Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The `strict` statement is available only for DHCPv6.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Options**
- `support-option-pd-exclude`—Request to exclude prefix option in the reconfigure message.

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

**RELATED DOCUMENTATION**
- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- DHCPv6 Prefix Exclusion
- `dhcp-attributes`
- `reconfigure` | 2168
reconfigure (DHCP Local Server)

Syntax

reconfigure {
 attempts number;
 clear-on-abort;
 strict;
 timeout number;
 token token-name;
 trigger {
    radius-disconnect;
 }
}

Hierarchy Level

[edit system services dhcp-local-server dhcpv6]
[edit system services dhcp-local-server group group-name]
[edit system services dhcp-local-server dhcpv6 group group-name]

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration.

Options

attempts number—Configure maximum number of attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Range: 1 through 10 attempts

Default: 8 attempts

clear-on-abort —Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

strict —Configure the system to only allow packets that contain the reconfigure accept option.
**timeout seconds**—Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

**Range:** 1 through 10 seconds  
**Default:** 2 seconds

**token token-name**—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

**trigger** — Specify DHCP reconfigure trigger.

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

---

**RELATED DOCUMENTATION**

| DHCP Overview | 909 |
| DHCP Server Configuration Overview | 916 |
redirect-url

Syntax

redirect-url url;

Hierarchy Level

[edit protocols dot1x authenticator interface interface-name]

Release Information
Statement introduced in Junos OS Release 15.1R3 for EX Series switches.

Description
Configure a URL that redirects unauthenticated hosts to a central Web authentication (CWA) server. The CWA server provides a web portal where the user can enter a username and password. If these credentials are validated by the CWA server, the user is authenticated and is allowed access to the network.

The redirect URL for central Web authentication can be configured centrally on the AAA server or locally on the switch. Use the `redirect-url` statement to configure the redirect URL locally on the interface connecting the host to the switch.

The redirect URL and a dynamic firewall filter must both be present for the central Web authentication process to be triggered. For more information about configuring the redirect URL and the dynamic firewall filter for central Web authentication, see "Configuring Central Web Authentication" on page 513.

Default
Disabled. The redirect URL is not enabled for central Web authentication by default.

Options
url—The URL that redirects the host to the server that will handle central web authentication. The redirect URL must use the HTTP or HTTPS protocol and include an IP address or website name. The following are examples of valid redirect URL formats:

- http://www.example.com
- https://www.example.com
- http://10.10.10.10
- https://10.10.10.10
- http://www.example.com/login.html
- https://www.example.com/login.html
NOTE: When the dynamic firewall filter is configured using the special Filter-ID attribute JNPR_RSVD_FILTER_CWA, the CWA redirect URL must include the IP address of the AAA server, for example, https://10.10.10.10.

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

RELATED DOCUMENTATION
- Configuring Central Web Authentication | 513
regex-additive-logic

Syntax

regex-additive-logic;

Hierarchy Level

[edit system]

Release Information


Description

Enable additive logic (that is, deny all by default / allow some as specified) to be used in regular expressions.

This statement changes the behavior of existing regular expressions so that all configuration hierarchies are denied by default and must be explicitly allowed using the allow-configuration-regexps statement.

For example, to grant users in a named user class access to a specific configuration hierarchy, but deny access to all other configuration hierarchies, enable the regex-additive-logic statement and configure an allow-configuration-regexps statement that includes the specific configuration hierarchy to which you want to allow access. When a user logs in, only the specified configuration hierarchy is visible.

Default

By default, this statement is disabled; configuration hierarchies not explicitly denied with a deny-configuration-regexps statement are visible to the user.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies  |  160
Example: Using Additive Logic With Regular Expressions to Specify Access Privileges  |  142
Regular Expressions for Allowing and Denying Junos OS Operational Mode Commands, Configuration Statements, and Hierarchies  |  128
class  |  1573
relay-agent-interface-id (DHCP Local Server)

Syntax

relay-agent-interface-id;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level

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

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients | 834
relay-agent-interface-id (DHCPv6 Relay Agent)

Syntax

```
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group ],
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description

Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

### RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-relay</td>
<td>1665</td>
</tr>
<tr>
<td>Extended DHCP Relay Agent Overview</td>
<td>792</td>
</tr>
<tr>
<td>DHCPv6 Relay Agent Overview</td>
<td>829</td>
</tr>
<tr>
<td>Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets</td>
<td>830</td>
</tr>
</tbody>
</table>
relay-agent-remote-id (DHCP Local Server)

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
For MX Series routers only, enterprise-id and remote-id options introduced in Junos OS Release 12.3R3.
For MX Series routers only, the enterprise-id and remote-id options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.

Description

Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.

Required Privilege Level

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

Creating Unique Usernames for DHCP Clients | 834
relay-agent-remote-id (DHCPv6 Relay Agent Username)

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
For MX Series routers only, enterprise-id and remote-id options introduced in Junos OS Release 12.3R3.
For MX Series routers only, the enterprise-id and remote-id options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description

 Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>DHCPv6 Relay Agent Overview</th>
<th>829</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating Unique Usernames for DHCP Clients</td>
<td>834</td>
</tr>
</tbody>
</table>
relay-option (DHCP Relay Agent)

Syntax

relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Configure the extended DHCP relay agent selective processing that is based on DHCP options in DHCP client packets and specify the action to perform on client traffic. You can configure support globally or for a named group of interfaces, and for either DHCP or DHCPv6 relay agent.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

* Using DHCP Option Information to Selectively Process DHCP Client Traffic
relay-option-82

Syntax

relay-option-82 {
    circuit-id {
        include-irb-and-l2;
        keep-incoming-circuit-id;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    server-id-override
    vendor-specific{
        host-name;
        location;
    }
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcprelay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
**Description**
Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

To enable insertion of option 82 information in DHCP packets, you must specify at least one of the `circuit-id` or `remote-id` statements.

You can use the `relay-option-82` statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level to control insertion of option 82 information globally, or at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level to control insertion of option 82 information for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), use the `delete relay-option-82` statement.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**
- Using DHCP Relay Agent Option 82 Information | 739
- dhcp-relay | 1665
relay-server-group (DHCP Relay Agent Option)

Syntax

```plaintext
relay-server-group relay-server-group;
```

Hierarchy Level

```plaintext
[edit forwarding-options dhcpv6 relay-option (default-action | equals | starts-with),
[edit forwarding-options dhcp relay-option (default-action | equals | starts-with),
[edit forwarding-options dhcp relay group group-name relay-option (default-action | equals | starts-with),
[edit forwarding-options dhcp relay dhcpv6 group group-name relay-option (default-action | equals | starts-with),
[edit logical-systems logical-system-name forwarding-options dhcpv6 relay-option (default-action | equals | starts-with),
[edit routing-instances routing-instance-name forwarding-options dhcpv6 relay-option (default-action | equals | starts-with),
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp relay-option (default-action | equals | starts-with),
[edit routing-instances routing-instance-name forwarding-options dhcp relay-option (default-action | equals | starts-with),
```

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Relay DHCP client packets to the specified group of DHCP servers when you use the DHCP relay selective processing feature. You can configure the relay operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Options

*relay-server-group*—Name of DHCP server group.

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

RELATED DOCUMENTATION

*Using DHCP Option Information to Selectively Process DHCP Client Traffic*
remote-debug-permission

Syntax

remote-debug-permission (qfabric-admin | qfabric-operator | qfabric-user);

Hierarchy Level

[edit system login user username authentication]
[edit system root-authentication]

Release Information

Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

(QFabric systems only) Configure authentication classes that permit or deny user access to individual components of the QFabric system.

Default

qfabric-user

Options

qfabric-admin—Permits a user to log in to individual QFabric system components, view operations, and change component configurations.

qfabric-operator—Permits a user to log in to individual QFabric system components and view component operations.

qfabric-user—Prevents a user from logging in to individual QFabric system components.

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Configuring QFabric System Login Classes

request component login | 2493

Understanding QFabric System Login Classes
remote-id (DHCP Relay Agent)

Syntax

remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
}

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ... relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82]

Release Information


Description

Specify the Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix, textual description, or VLAN tag.

NOTE: For Layer 3 interfaces, when you configure relay-option-82 only, the Agent Remote ID is the default. If no VLAN tags are configured, then the default is the logical interface device (IFL) name. For integrated routing and bridging (IRB) interfaces, the default is the Layer 2 IFL name and bridge domain name.

The interface to bridge domain relationship may be implicit (the interface is mapped to the bridge domain by the system based on VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.
The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs), stacked VLANs (S-VLANs), or bridge domains is as follows:

(fe | ge)-fpc/pic/port.subunit

**NOTE:** For remote systems, the *subunit* is required and is used to differentiate an interface.

The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

(fe | ge)-fpc/pic/port:vlan-id

The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

(fe | ge)-fpc/pic/port:svlan-id--vlan-id

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-fpc/pic/port:bridge-domain-name

- IRB interfaces that use VLANs:

  (fe | ge)-fpc/pic/port:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the `include-irb-and-l2` statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

  (fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

  (fe | ge)-fpc/pic/port:vlan-name+irb.subunit
To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

```
irb.subunit
```

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Using DHCP Relay Agent Option 82 Information | 739
- Configuring Option 82 Information
replace-ip-source-with (DHCP Relay Agent)

Syntax

replace-ip-source-with giaddr;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides]

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

Required Privilege Level

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

RELATED DOCUMENTATION

overrides (DHCP Relay Agent) | 2050
replace-ip-source-with (DHCP Relay Agent)

Syntax

replace-ip-source-with giaddr;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

Required Privilege Level

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

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview | 792
Replacing the DHCP Relay Request and Release Packet Source Address | 796
req-option

Syntax

req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.
The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description

The configuration options requested by the DHCPv6 client.

Options

dns-server—Specify a DNS server.
domain—Specify a domain name.
fqdn—Specify a fully qualified domain name.
nis-domain—Specify a Network Information Service (NIS) domain.
nis-server—Specify a Network Information Service (NIS) server.
ntp-server—Specify a Network Time Protocol (NTP) server.
sip-domain—Specify a Session Initiation Protocol (SIP) domain.
sip-server—Specify a Session Initiation Protocol (SIP) server.
time-zone—Specify a time zone.
vendor-spec—Specify vendor specification.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
retransmission-attempt (DHCP Client)

Syntax

```
retransmission-attempt number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

Release Information

Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the number of times the device retransmits a Dynamic Host Control Protocol (DHCP) packet if a DHCP server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options

- **number**—Number of retransmit attempts.

Range: 0 through 6
Default: 4

Required Privilege Level

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

RELATED DOCUMENTATION

| Configuring a DHCP Client (CLI Procedure) | 762 |
| interfaces |
| unit |
| family |
retransmission-attempt (DHCP Client)

Syntax

retransmission-attempts number;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcp-client]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-clinet at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

Description
Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.

Options
number—Number of attempts to retransmit the packet.

Range: 0 through 6

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

RELATED DOCUMENTATION

| Understanding DHCP Client Operation | 933 |
| Minimum DHCP Client Configuration | 934 |
retransmission-attempt (DHCPv6 Client)

Syntax

retransmission-attempt number;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]

Release Information
Statement introduced in Junos OS Release 12.1X45-D10.
The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description
Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options
number—Number of retransmit attempts

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

RELATED DOCUMENTATION
retransmission-interval (DHCP Client)

Syntax

retransmission-interval  seconds;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet dhcp]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.

Options
- **seconds**—Number of seconds between successive retransmissions.

Range: 4 through 64 seconds

Default: 4 seconds

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

RELATED DOCUMENTATION

- Configuring a DHCP Client (CLI Procedure) | 762
retransmission-interval (DHCP Client)

Syntax

```
retransmission-interval seconds;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family-name dhcp]
```

Release Information

Statement introduced in Release 8.5 of Junos OS.

Description

Specify the time between successive retransmission attempts.

Options

- **seconds**—Number of seconds between successive retransmission.

Range: 4 through 64 seconds

Default: 4 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- Junos OS Initial Configuration Guide for Security Devices
retransmission-interval (DHCP Client)

Syntax

retransmission-interval seconds;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcp-client]

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-clinet at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

Description

Specify the initial retransmission interval. Successive retransmission intervals are doubled as per RFC2131.

NOTE: Though the SRX series devices implement the exponential backoff, as described in RFC 2131, the retransmit attempt does not stop when the retransmission interval reaches 64 seconds. The packet is transmitted till the retransmission attempt is reached. For example, if you configure the retransmission-attempt to 5 and the retransmission-interval to 20, the sequence of retransmission-interval is 20, 40, 80, 160, 320.

Options

seconds—Number of seconds before initial retransmission.

Range: The range is 4 through 64. The default is 4 seconds.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Understanding DHCPv6 Client and Server Identification | 1005 |
retries (802.1X)

Syntax

retries number;

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [interface-names])]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
For 802.1X authentication, configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

Options
number—Number of retries.

Default: 3 retries

Range: 1 through 10

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

RELATED DOCUMENTATION

Configuring 802.1X Interface Settings (CLI Procedure) | 390

Configuring 802.1X Authentication (J-Web Procedure)

Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients | 415
retries (Captive Portal)

Syntax

retries number-of-tries;

Hierarchy Level

[edit services captive-portal interface (all | interface-names)]

Release Information
Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description
Configure the number of times the user can attempt to submit authentication information.

Options

number-of-tries—Number of authentication attempts by user.

Range: 1–65535
Default: 3

Required Privilege Level
routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

RELATED DOCUMENTATION

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Configuring Captive Portal Authentication (CLI Procedure) | 492
retry

Syntax

retry number;

Hierarchy Level

[edit system radius-server server-address],
[edit system accounting destination radius server server-address]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.

Options
number—Number of retries allowed for contacting a RADIUS server.

Range: 1 through 10
Default: 3

NOTE: The [edit system accounting] hierarchy is not available on QFabric systems.

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

RELATED DOCUMENTATION

Configuring RADIUS Authentication (QFX Series or OCX Series) | 244

timeout
retry (RADIUS)

Syntax

    retry number;

Hierarchy Level

    [edit system radius-server server-address],
    [edit system accounting destination radius server server-address]

Release Information

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

Description

Number of times the router or switch is allowed to try to contact a RADIUS authentication or accounting server.

Options

    number—Number of retries allowed for contacting a RADIUS server.

Range: 1 through 10
Default: 3

Required Privilege Level

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

RELATED DOCUMENTATION

    Configuring RADIUS Server Authentication  |  233
    Configuring RADIUS System Accounting  |  255
    timeout  |  2324
retry-options

Syntax

```bash
retry-options {
    backoff-factor seconds;
    backoff-threshold number;
    maximum-time seconds;
    minimum-time seconds;
    tries-before-disconnect number;
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
**maximum-time** option introduced in Junos OS Release 9.6.
**maximum-time** option introduced in Junos OS Release 9.6 for EX Series switches.

Description

Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.

Required Privilege Level

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

RELATED DOCUMENTATION

- Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82
- rate-limit | 2162
- lockout-period | 1920
revert-interval (Access)

Syntax

```plaintext
revert-interval interval;
```

Hierarchy Level

```
[edit access profile profile-name radius options],
[edit access radius-options]
```

Release Information

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

Description

Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.

Options

- `interval`—Amount of time to wait.

Range: 0 through 604,800 seconds

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- RADIUS Servers and Parameters for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access


rising-threshold (Health Monitor)

Syntax

rising-threshold percentage;

Hierarchy Level

[edit snmp health-monitor]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Set the upper threshold for the monitored object when you configure a health monitor alarm. By setting a rising and a falling threshold for a monitored object, you can be alerted whenever the value of the variable falls outside the allowable operational range.

Options

percentage—Upper threshold for the alarm entry.

Range: 1 through 100
Default: 80 percent of the maximum possible value

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Health Monitoring

falling-threshold | 1784
rng

Syntax

rng

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 18.3R1.
HMAC DRBG option introduced in Junos OS Release 18.3R1 for non-FIPS mode also.
dyce option introduced in Junos OS Release 19.3R1.

Description

Configure a system cryptographically secure pseudorandom number generator (CSPRNG). By default rng is not configured.

NOTE: Only root users can configure rng options.

A device reboot is required for the change to take effect.

In FIPS mode, HMAC-DRBG will be the only active RNG available.

Default

Options

fortuna—Configure the fortuna CSPRNG.

hmac-drbg—Configure the HMAC DRBG CSPRNG.

dyce—Configure the DYCE CSPRNG.

Required Privilege Level

system—To view this statement in the configuration.
root-authentication

Syntax

```
root-authentication {
    encrypted-password "password";
    no-public-keys
    ssh-ecdsa name {
        from from;
    }
    ssh-ed25519 name {
        from from;
    }
    ssh-rsa name {
        from from;
    }
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 8.5 for SRX Series.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the authentication methods for the root-level user, whose username is root.

You can use the ssh-ecdsa, ssh-ed25519, or ssh-rsa statements to directly configure SSH ECDSA, ED25519, or RSA keys to authenticate root logins. You can configure more than one public key for SSH authentication of root logins as well as for user accounts. When a user logs in as root, the public keys are referenced to determine whether the private key matches any of them.

Options

encrypted-password "password"—Specify the MD5 or other password. You can specify only one encrypted password. You cannot configure a blank password using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.
no-public-keys—Disable SSH public key-based authentication.

ssh-ecdsa name from from—Use an SSH ECDSA public key. You can specify one or more public keys.

ssh-ed25519 name from from—Use an SSH ED25519 public key. You can specify one or more public keys.

ssh-rsa name from from—Use an SSH RSA public key. You can specify one or more public keys.

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

RELATED DOCUMENTATION

| class (Defining Login Classes) | 1573 |
| user (Access) | 2402 |
root-login

Syntax

root-login (allow | deny | deny-password);

Hierarchy Level

[edit system services ssh]

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

Description
Control user access through SSH.

Default
root-login deny-password is the default for most systems.

Starting in Junos release 17.4R1 for MX Series routers, the default for root-login is deny. In previous Junos releases, the default setting for the MX240, MX480, MX960, MX2010 and MX2020 was allow.

Options
allow—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

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

RELATED DOCUMENTATION

Configuring SSH Service for Remote Access to the Router or Switch | 294
route-suppression (DHCP Local Server and Relay Agent)

Syntax

route-suppression (access | access-internal | destination);

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name ...],
[edit routing-instances routing-instance-name ...],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name]

Release Information

Statement introduced in Junos OS Release 13.2.

Description

Configure the jdhcpd process to suppress the installation of access, access-internal, or destination routes during client binding.

NOTE: You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.

Options

access—(DHCPv6 only) Suppress installation of access routes. You can use the access and access-internal options in the same statement for DHCPv6.

access-internal—In a DHCPv4 hierarchy, suppress installation of both access-internal and destination routes. In a DHCPv6 hierarchy, suppress access-internal routes only. Can be configured in the same statement with the access option.
**destination**—(DHCPv4 only) Suppress installation of destination routes. This option and the **access-internal** option are mutually exclusive; however, the **access-internal** option also suppresses destination routes.

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

**RELATED DOCUMENTATION**
- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | 897
routing-engine-profile

Syntax

```
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

Hierarchy Level

```
[edit accounting-options]
```

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

Description
Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the `/var/log` directory.

Options
- `profile-name`—Name of the Routing Engine statistics profile.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

- Configuring the Routing Engine Profile
routing-instance

Syntax

```text
routing-instance {
    instance-name {
        bridge-domain bridge-domain-name;
    }
    vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

- [edit forwarding-options analyzer analyzer-name input egress]
- [edit forwarding-options analyzer analyzer-name input ingress]
- [edit forwarding-options analyzer analyzer-name output]

Release Information


Description

Configure routing instance.

Options

- `instance-name`—Name of the routing instance.

Required Privilege Level

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

RELATED DOCUMENTATION
routing-instance-name (DHCP Local Server)

Syntax

```
 routing-instance-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
```

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

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

**RELATED DOCUMENTATION**
- Using External AAA Authentication Services with DHCP | 833
routing-instance-name (DHCP Relay Agent)

Syntax

routing-instance-name;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit tenants tenant-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include]
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.
The tenants option is introduced in Junos OS Release 18.4R1.
Description
Specify that the routing instance name is concatenated with the username during the subscriber authentication or client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

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

RELATED DOCUMENTATION
- Using External AAA Authentication Services with DHCP | 833
- Creating Unique Usernames for DHCP Clients | 834
secret (RADIUS or TACACS+ Server)

Syntax

```
secret password;
```

Hierarchy Level

```
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address],
[edit system radius-server server-address],
[edit system tacplus-server server-address]
```

Release Information

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

Description

Configure the password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server.

**NOTE:** To ensure better security, we recommend you to configure TACACS+ secret password with a minimum of 14 characters.

Options

- **password**—Password to use; can include spaces included in quotation marks.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
- Configuring TACACS+ Authentication | 264
- Configuring TACACS+ System Accounting | 278
- Configuring RADIUS System Accounting | 255
secret (RADIUS)

Syntax

secret password;

Hierarchy Level

[edit access profile profile-name radius-server server-address],
[edit access radius-disconnect client-address],
[edit access radius-server server-address]

Release Information

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

Description

Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

Options

password—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Authentication and Accounting Parameters for Subscriber Access
RADIUS Authentication and Accounting Server Definition
Example: Configuring CHAP Authentication with RADIUS
Configuring RADIUS Authentication for L2TP
Configuring the RADIUS Disconnect Server for L2TP
secret (Security)

Syntax

```plaintext
secret secret-data;
```

Hierarchy Level

```plaintext
[edit security authentication-key-chains key-chain key-chain-name key key]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

Options

`secret-data`—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols | 286
- Example: Configuring BFD Authentication for Securing Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS
secure-authentication

Syntax

secure-authentication (http | https);

Hierarchy Level

[edit services captive-portal]

Release Information
Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description
Enable HTTP or HTTPS access on the captive portal interface.

Default
http

Options
http—Enables HTTP access on the captive portal interface.

https—Enables HTTPS access on the captive portal interface. HTTPS is recommended.

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

RELATED DOCUMENTATION

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Configuring Captive Portal Authentication (CLI Procedure) | 492
security

Syntax

```plaintext
security {
    authentication-key-chains {
        key-chain key-chain-name {
            key key {
                secret secret-data;
                start-time yyyy-mm-dd.hh:mm:ss;
            }
        }
    }
}

certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
        ca-name ca-identity;
        crl file-name;
        encoding (binary | pem);
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
    enrollment-retry attempts;
    local certificate-filename {
        certificate-key-string;
        load-key-file key-file-name;
    }
    maximum-certificates number;
    path-length certificate-path-length;
}

ssh-known-hosts {
    host {
        fetch-from-server host-name;
        load-key-file file-name;
    }
}

traceoptions {
    file filename <files number> <size size>;
    flag flag;
    level level;
    no-remote-trace
}
}
```
Hierarchy Level

[edit]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description
Configure security services. Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

Required Privilege Level

RELATED DOCUMENTATION

send-acct-status-on-config-change (Access Profile)

Syntax

send-acct-status-on-config-change;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure the router's authd process to send accounting messages when the RADIUS server status changes for an access profile. When you include this statement, authd sends an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.

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

RELATED DOCUMENTATION

Configuring Per-Subscriber Session Accounting
RADIUS Servers and Parameters for Subscriber Access
send-release-on-delete (DHCP Relay Agent)

Syntax

```
send-release-on-delete;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]
```

Release Information

Statement introduced in Junos OS Release 10.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Send a release message to the DHCP (or DHCPv6) server whenever DHCP relay or relay proxy deletes a client. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

Required Privilege Level

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

RELATED DOCUMENTATION

| Extended DHCP Relay Agent Overview  | 792 |
| Overriding the Default DHCP Relay Configuration Settings  | 803 |
| Sending Release Messages When Clients Are Deleted  | 840 |
server (NTP)

Syntax

```
server address <key key-number> <version value> <prefer>;
```

Hierarchy Level

```
[edit system ntp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For NTP, configure the SRX Series device to operate in client mode with the remote system at the specified address. In this mode, the SRX Series device can be synchronized with the remote system, but the remote system can never be synchronized with the SRX Series device.

If the NTP client time drifts so that the difference in time from the NTP server exceeds 128 milliseconds, the client is automatically stepped back into synchronization. If the offset between the NTP client and server exceeds the 1000-second threshold, the client still synchronizes with the server, but it also generates a system log message noting that the threshold was exceeded.

Options

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

- **key key-number**—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.

  Range: Any unsigned 32-bit integer

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

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

  Range: 1 through 4

  Default: 4

Required Privilege Level

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

ntp | 2005
server (DNS, Port, and TFTP Service)

Syntax

```bash
server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
```

Hierarchy Level

- [edit forwarding-options helpers domain],
- [edit forwarding-options helpers domain interface interface-name],
- [edit forwarding-options helpers port port-number],
- [edit forwarding-options helpers port port-number interface interface-name],
- [edit forwarding-options helpers tftp],
- [edit forwarding-options helpers tftp interface interface-name]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced for port helpers in Junos OS Release 17.2R1 for EX4300 switches.
- Support for multiple server instances for a given port introduced in Junos OS Release 17.2 for MX Series routers.
- Support for multiple server instances for a given port introduced in Junos OS Release 17.3R1 for EX9200 switches.

Description

Specify the DNS or TFTP server for forwarding DNS or TFTP requests, or specify a destination server address for forwarding LAN broadcast packets as unicast traffic for a custom-configured UDP port.

When configuring port helpers, in releases prior to Junos OS Release 17.2, only one server can be specified for a given port. For Junos OS Release 17.2 and later, multiple servers can be specified for a given port at the global or interface-specific level. When multiple servers are specified, the same packet, with the originator IP address and port requests, is forwarded to the different configured servers; the payload of the UDP packet is not modified.

Options

- `address`—IP address of the server.
- `logical-system logical-system-name`—(Optional) Logical system name of the server.
- `routing-instance [ routing-instance-names ]`—(Optional) Set the routing instance name or names that belong to the DNS server or TFTP server.

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

RELATED DOCUMENTATION

- Configuring DNS and TFTP Packet Forwarding
- Configuring Port-based LAN Broadcast Packet Forwarding
server (RADIUS Accounting)

Syntax

server {
    server-address {
        accounting-port port-number;
        retry number;
        routing-instance routing-instance;
        secret password;
        source-address address;
        timeout seconds;
    }
}

Hierarchy Level

[edit system accounting destination radius]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the source-address-inet6 statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Configure RADIUS logging.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS System Accounting | 255
server (TACACS+ Accounting)

Syntax

```
server {
    server-address {
        port port-number;
        routing-instance (Accounting and Authentication) routing-instance;
        secret password;
        single-connection;
        timeout seconds;
    }
}
```

Hierarchy Level

```
[edit system accounting destination tacplus]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
`routing-instance` option introduced in Junos OS Release 17.4R1.

Description

Configure TACACS+ logging.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

| Configuring TACACS+ System Accounting | 278 |
server-address

Syntax

server-address  ip-address;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet dhcp]

Release Information

Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the address of the DHCP server that the client should accept DHCP offers from. If this option is included in the DHCP configuration, the client accepts offers only from this server and ignores all other offers.

Default

The client accepts the first offer it receives from any DHCP server.

Options

ip-address—DHCP server address.

Required Privilege Level

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

RELATED DOCUMENTATION

| Configuring a DHCP Client (CLI Procedure) | 762 |
| interfaces |
| unit |
| family |
server-address (dhcp-client)

Syntax

server address ip-address;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcp-client]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-clinet at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

Description
Specify the preferred DHCP server address that is sent to DHCP clients.

Options
ip-address—DHCP server address.

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

RELATED DOCUMENTATION
server-fail

Syntax

```
server-fail (deny | permit | use-cache | vlan-id | vlan-name);
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (all | [interface-names])]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure authentication fallback options to specify how end devices connected to a switch are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant’s initial attempt at authentication through the RADIUS server.

When you configure the server fail fallback feature you must specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch.

**NOTE:** The `server-fail` statement is specifically for data traffic. For VoIP tagged traffic, use the `server-fail-voip` statement. The same interface can have a `server-fail` VLAN and a `server-fail-voip` VLAN configured.

Default

If the `server-fail` statement is not configured, in the event that the RADIUS authentication server becomes unavailable, the end device is not authenticated and is denied access to the network.

Options

deny—Force fail the supplicant authentication. No traffic will flow through the interface.

permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.
**use-cache**—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected.

**vlan-id**—Move supplicant on the interface to the VLAN specified by this numeric identifier. This action is allowed only if it is the first supplicant connecting to the interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

**vlan-name**—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x</td>
<td>2644</td>
</tr>
<tr>
<td>Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch</td>
<td>408</td>
</tr>
<tr>
<td>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</td>
<td>400</td>
</tr>
<tr>
<td>Configuring RADIUS Server Fail Fallback (CLI Procedure)</td>
<td>384</td>
</tr>
<tr>
<td>Understanding Server Fail Fallback and Authentication on Switches</td>
<td>383</td>
</tr>
</tbody>
</table>
server-fail-voip

Syntax

server-fail (deny | permit | use-cache | vlan-name);

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names])]

Release Information
Statement introduced in Junos OS Releases 14.1X53-D40 and 15.1R4 for EX Series switches.

Description
Configure authentication fallback options to specify how VoIP clients sending voice traffic are supported if the RADIUS authentication server becomes unavailable. Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by a supplicant’s initial attempt at authentication through the RADIUS server.

When you configure the server fail fallback feature you must specify an action that the switch applies to end devices when the authentication servers are unavailable. The switch can accept or deny access to supplicants or maintain the access already granted to supplicants before the RADIUS timeout occurred. You can also configure the switch to move the supplicants to a specific VLAN. The VLAN must already be configured on the switch.

The server-fail-voip statement is specific to the VoIP-tagged traffic sent by clients. VoIP clients still require that the server-fail statement be configured for the un-tagged traffic that they generate. Therefore, when you configure the server-fail-voip statement you must also configure the server-fail statement.

NOTE: An option other than server-fail deny must be configured for server-fail-voip to successfully commit.

Default
If the server-fail-voip statement is not configured, in the event that the RADIUS authentication server becomes unavailable, a VoIP client that begins authentication by sending voice traffic is not authenticated, and the voice traffic is dropped.

Options
deny—Force fail the supplicant authentication. No traffic will flow through the interface.
permit—Force succeed the supplicant authentication. Traffic will flow through the interface as if it were successfully authenticated by the RADIUS server.

use-cache—Force succeed the supplicant authentication only if it was previously authenticated successfully. This action ensures that already authenticated supplicants are not affected. This option can be used only for reauthentication.

vlan-name—Move supplicant on the interface to the VLAN specified by this name. This action is allowed only if it is the first supplicant connecting to an interface. If an authenticated supplicant is already connected, then the supplicant is not moved to the VLAN and is not authenticated. The VLAN must already be configured on the switch.

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

RELATED DOCUMENTATION

| show dot1x | 2644 |
| Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 408 |
| Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400 |
| Configuring RADIUS Server Fail Fallback (CLI Procedure) | 384 |
| Understanding Server Fail Fallback and Authentication on Switches | 383 |
server-group

Syntax

server-group {
  server-group-name {
    server-ip-address;
  }
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6]

Release Information
Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Apply the group with the active-server-group statement globally for all interfaces or for a named group of interfaces configured with the group statement. This mechanism enables you to apply different DHCP relay configurations for different groups of servers, with a common configuration for the servers within a server group.

Options

server-group-name—Name of the group of DHCP or DHCPv6 server addresses.

server-ip-address—IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. Starting in Junos OS Release 18.4R1, you can configure up to 32 server IP addresses per group for DHCPv4 servers. In earlier releases, you can configure only up to 5 server IP addresses for DHCPv4 servers. For DHCPv6 servers, you can configure only up to 32 addresses in all releases. The configuration fails commit check if you configure more than the maximum number of server addresses.
Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Extended DHCP Relay Agent Overview</th>
<th>792</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups</td>
<td>850</td>
</tr>
</tbody>
</table>
server-identifier

Syntax

server-identifier address;

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

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

Description

Configure a server identifier. The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

Servers include the server identifier in **DHCPoffer** messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in **DHCPREQUEST** messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.

This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.

Default

If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on **fe-0/0/0** and the primary interface address is **1.1.1.1**, then the server identifier is set to **1.1.1.1**.

Options

**address**—IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

Required Privilege Level

system—To view this statement in the configuration.

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

Syntax

```
server-reject-vlan (vlan-id | vlan-name) {
    eapol-block;
    block-interval block-interval;
}
```

Hierarchy Level

```
[edit protocols dot1x authenticator interface (802.1X) (all | [interface-names])]
```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description

For EX Series switches configured for 802.1X authentication, specify that when the switch receives an Extensible Authentication Protocol Over LAN (EAPoL) Access-Reject message during the authentication process between the switch and the RADIUS authentication server, supplicants attempting access to the LAN are granted access and moved to a specific VLAN. Any VLAN name or VLAN ID sent by a RADIUS server as part of the EAPoL Access-Reject message is ignored.

When you specify the VLAN ID or VLAN name, the VLAN must already be configured on the switch.

The remaining statements are explained separately. See CLI Explorer.

Default

None

Options

- **vlan-id**—Numeric identifier of the VLAN to which the supplicant is moved.
- **vlan-name**—Name of the VLAN to which the supplicant is moved.

Required Privilege Level

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

RELATED DOCUMENTATION

- `show dot1x` | 2644
<table>
<thead>
<tr>
<th>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</th>
<th>400</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients</td>
<td>415</td>
</tr>
<tr>
<td>Configuring RADIUS Server Fail Fallback (CLI Procedure)</td>
<td>384</td>
</tr>
<tr>
<td>Understanding Server Fail Fallback and Authentication on Switches</td>
<td>383</td>
</tr>
</tbody>
</table>
server-timeout

Syntax

server-timeout seconds;

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [interface-name])

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

For 802.1X authentication, configure the amount of time a port will wait for a reply when relaying a response from the supplicant to the authentication server before timing out and invoking the server-fail action.

Default

30 seconds

Options

seconds — Number of seconds.

Range: 1 through 60 seconds

Default: 30 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

| show dot1x | 2644 |
| clear dot1x | 2477 |

Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400
802.1X for Switches Overview | 387
server-timeout (Captive Portal)

Syntax

```
server-timeout seconds;
```

Hierarchy Level

```
[edit services captive-portal interface (all | interface-names)]
```

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description

Configure the time in seconds an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.

Options

- `seconds`—Number of seconds.

Range:  1–65535

Default: 20

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing–control`—To add this statement to the configuration.

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Example: Setting Up Captive Portal Authentication on an EX Series Switch</th>
<th>485</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Captive Portal Authentication (CLI Procedure)</td>
<td>492</td>
</tr>
</tbody>
</table>
servers

Syntax

```
servers server-address {
    port port-number;
}
```

Hierarchy Level

```
[edit system services service-deployment]
```

Release Information

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

Description

Configure an IPv4 address for the Session and Resource Control (SRC) server.

Options

- `server-address`—The TCP port number.

Default: 3333

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Junos OS to Work with SRC Software
service (Service Accounting)

Syntax

```plaintext
service {
    accounting-order (activation-protocol | local | radius);
    accounting {
        statistics (time | volume-time);
        update-interval minutes;
    }
}
```

Hierarchy Level

```
[edit access profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
`accounting`, `update-interval`, and `statistics` options added in Junos OS Release 14.2R1 for MX Series routers.

Description

Define the subscriber service accounting configuration.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Service Accounting with JSRC
- Service Accounting with JSRC
- Configuring Service Accounting in Local Flat Files
- Configuring Service Accounting
- Configuring Per-Subscriber Session Accounting
service-deployment

Syntax

```bash
service-deployment {
  servers server-address {
    port port-number;
  }
  source-address source-address;
}
```

Hierarchy Level

[edit system services]

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

Description
Enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

- Configuring the Junos OS to Work with SRC Software
service-profile (DHCP Local Server)

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

- [edit system services dhcp-local-server],
- [edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
- [edit system services dhcp-local-server dhcpv6],
- [edit system services dhcp-local-server dhcpv6 group group-name],
- [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
- [edit system services dhcp-local-server group group-name],
- [edit system services dhcp-local-server group group-name interface interface-name],
- [edit logical-systems logical-system-name system services dhcp-local-server ...],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
- [edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the default subscriber service or DHCP client management service, which is activated when the subscriber or client logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP local server clients, include the `service-profile` statement at the [edit system services dhcp-local-server] hierarchy level.
- To specify the default service for a named group of interfaces, include the `service-profile` statement at the [edit system services dhcp-local-server group group-name] hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the `service-profile` statement at the [edit system services dhcp-local-server group group-name interface interface-name] hierarchy level.
- For DHCPv6 clients, use the `service-profile` statement at the [edit system services dhcp-local-server dhcpv6] hierarchy level.

Options

- **dynamic-profile-name**—Name of the dynamic profile that defines the service.
Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Extended DHCP Local Server Overview | 718
- Default Subscriber Service Overview
- Configuring a Default Subscriber Service
**service-profile (DHCP Relay Agent)**

**Syntax**

```
service-profile dynamic-profile-name;
```

**Hierarchy Level**

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

**Release Information**

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

**Description**

Specify the default subscriber service (or the default DHCP client management service), which is activated when the subscriber (or client) logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP relay agent clients, include the `service-profile` statement at the [edit forwarding-options dhcp relay] hierarchy level.
- To specify the default service for a named group of interfaces, include the `service-profile` statement at the [edit forwarding-options dhcp relay group group-name] hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the `service-profile` statement at the [edit forwarding-options dhcp relay group group-name interface interface-name] hierarchy level.

**Options**
**dynamic-profile-name**—Name of the dynamic service profile.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>dhcp-relay</th>
<th>1665</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Grouping Interfaces with Common DHCP Configurations</strong></td>
<td>853</td>
</tr>
<tr>
<td><strong>Default Subscriber Service Overview</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Configuring a Default Subscriber Service</strong></td>
<td></td>
</tr>
</tbody>
</table>
services (System Services)

Syntax

services {
    dhcp { # DHCP is not supported on a DCF
        dhcp_services;
    }
    dtcp-only
    flow-tap-dtcp {
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
    extension-service {
        request-response {
            grpc {
                ssl {
                    address ip-address;
                    local-certificate local-certificate;
                    port port;
                }
                max-connections max-connections;
            }
        }
        notification {
            port port;
            max-connections max-connections;
            allow-clients {
                address ip-address;
            }
        }
        traceoptions {
            file <filename> <files number> <match regex> <size size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
    }
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    ftp {
    }
}
authentication-order [authentication-methods];
connection-limit limit;
rate-limit limit;
}
service-deployment {
    servers address {
        port-number port-number;
    }
    source-address address;
}
ssh {
    authentication-order [authentication-methods];
ciphers [cipher-1 cipher-2 cipher-3 ...];
    client-alive-count-max seconds;
    client-alive-interval seconds;
    connection-limit limit;
    fingerprint-hash (md5 | sha2-256);
    hostkey-algorithm (algorithm | no-algorithm);
    key-exchange [algorithm];
    macs [algorithm];
    max-sessions-per-connection <number>;
    no-passwords;
    no-public-keys;
    no-tcp-forwarding;
    protocol-version [v1 v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
    sftp-server;
}
resource-monitor {
    free-fw-memory-watermark number;
    free-heap-memory-watermark number;
    free-nh-memory-watermark number;
    high-threshold number;
    no-logging;
    no-throttle;
    resource-category jtree {
        resource-type (contiguous-pages | free-dwords | free-pages) {
            low-watermark number;
            high-watermark number;
        }
    }
    subscribers-limit {
        client-type (any | dhcp | l2tp | pppoe) {
            chassis {
                limit limit;
            }
            fpc slot-number {
                limit limit;
                pic number {
                    limit limit;
                    port number {
                        limit limit;
                    }
                }
            }
        }
    }
    traceoptions {
        file filename <files number> <match regular-expression> <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
subscriber-management {
    enable;
    enforce-strict-scale-limit-license;
    gres-route-flush-delay;
}
overrides {
    event {
        catastrophic-failure {
            reboot (master | standby);
        }
    }
    interfaces {
        family (inet | inet6) {
            layer2-liveness-detection;
        }
    }
    no-unsolicited-ra;
    ra-initial-interval-max seconds;
    ra-initial-interval-min seconds;
    shmlog {
        disable;
        file filename <files maximum-no-files> <size maximum-file-size>;
        filtering enable;
        log-name {
            all;
            logname {
                <brief | detail | extensive | none | terse>;
                <file-logging | no-file-logging>;
            }
        }
        log-type (debug | info | notice);
    }
    redundancy {
        interface name {
            virtual-inet-address virtual-v4-address;
            virtual-inet6-address virtual-v6-address;
        }
        no-advertise-routes-on-backup;
        protocol vrrp;
    }
    traceoptions {
        file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable | no-world-readable>;
flag flag;
}
}
telnet {
  authentication-order [authentication-methods];
  connection-limit limit;
  rate-limit limit;
}
web-management {
  http {
    interfaces [names ];
    port port;
  }
  https {
    interfaces [names ];
    local-certificate name;
    port port;
  }
  session {
    idle-timeout [minutes ];
    session-limit [limit ];
  }
}
}
xml-ssl {
  connection-limit limit;
  local-certificate name;
  rate-limit limit;
  ssl-renegotiation;
}
}

Hierarchy Level

[edit system]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description
Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, DTCP over SSH, finger, rlogin, SSH, telnet, Web management, Junos XML protocol SSL, and network utilities, or enable Junos OS to work with the Session and Resource Control (SRC) software. Also, enable configuration of third-party applications developed using the Juniper Extension Toolkit (JET) to run on Junos OS.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level
system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Configuring the Junos OS to Work with SRC Software
- Understanding JET Interaction with Junos OS
- Configuring Junos OS Enhanced Subscriber Management
- How to Configure M:N Subscriber Redundancy with DHCP Binding Synchronization
services (Switches)

Syntax

services {
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        connection-limit limit;
        protocol-version [v1 v2];
        rate-limit limit;
        root-login (allow | deny | deny-password);
    }
}

Hierarchy Level

[edit system]

Release Information

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

Description

Configure the switch so that users on remote systems can access the local switch through SSH.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
session (Time-out)

Syntax

```
session {
    idle-timeout minutes;
    session-limit session-limit;
}
```

Hierarchy Level

```
[edit system services web-management]
```

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

Options

- `idle-timeout minutes`—Configure the number of minutes a session can be idle before it times out.
  - Range: 1 through 1440
  - Default: 1440

- `session-limit session-limit`—Configure the maximum number of simultaneous J-Web user login sessions.
  - Range: 1 through 1024
  - Default: Unlimited

Required Privilege Level

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

RELATED DOCUMENTATION

- J-Web Interface User Guide
session-expiry

Syntax

```
session-expiry seconds;
```

Hierarchy Level

```
[edit services captive-portal interface (all | interface-names)]
```

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description

The `session-expiry` statement is used to locally configure the number of seconds before the captive portal authentication session times out and the client must reattempt authentication.

**NOTE:** If the authentication server sends an authentication session timeout to the client, this takes priority over the value configured locally using the `session-expiry` statement. The session timeout value is sent from the server to the client as an attribute of the RADIUS Access-Accept message.

Options

- `seconds`—Duration of session.

Range: 1 through 65535

Default: 3600

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492
- Understanding Authentication Session Timeout | 370
session-mode

Syntax

session-mode (automatic | multihop | singlehop);

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the session mode.

Options
Default: automatic

automatic—Configure single-hop BFD sessions if the peer is directly connected to the router interface and multihop BFD sessions if the peer is not directly connected to the router interface.

multihop—Configure multihop BFD sessions and passive DHCP clients.

single-hop—Configure single hop BFD sessions and non-passive DHCP clients.

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

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients  |  869
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients  |  862
sftp-server

Syntax

sftp-server;

Hierarchy Level

[edit system services ssh]

Release Information

Statement introduced in Junos OS Release 19.1R1.

Description

Globally enable incoming SSH File Transfer Protocol (SFTP) connections. By setting `sftp-server` you enable authorized devices to connect to the device through SFTP. If `sftp-server` is not present, then SFTP is globally disabled and no devices can connect to the device through SFTP.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
short-cycle-protection (DHCP Local Server and Relay Agent)

Syntax

```
short-cycle-protection <lockout-max-time seconds> <lockout-min-time seconds>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name]
[edit logical-systems name forwarding-options dhcp-relay ...],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay ...],
[edit routing-instances name forwarding-options dhcp-relay ...],
[edit logical-systems name system services dhcp-local-server ...],
[edit logical-systems name routing-instances name system services dhcp-local-server dhcp-local-server ...],
[edit routing-instances name system services dhcp-local-server ...],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 18.2R1 on MX Series routers.

Description

Enable DHCP short-cycle protection to reduce resource usage associated with connection and authentication processing in highly scaled networks. You must configure both the minimum duration and the maximum duration for the lockout period.

The router detects short-lived client sessions and clients that repeatedly fail session negotiation, then locks them out from access by dropping subsequent DHCP discover or solicit messages from the client. The clients are tracked by the client identifier (client key), which can be a MAC address or some other unique value for DHCPv4 clients or the DUID for DHCPv6 clients. Locked-out clients are entered in the
lockout database. If a locked-out client attempts another session before the grace time threshold is reached, it is locked out again. Each successive lockout period is increased exponentially up to the maximum lockout period. The grace time threshold is automatically set at whichever value is larger, 900 seconds or the configured maximum value.

Options

**lockout-max-time seconds**—Maximum length of any lockout period; the upper bound of the lockout range.

- **Range:** 1 through 86400

**lockout-min-time seconds**—Minimum length of any lockout period; the lower bound of the lockout period.

- The minimum value is the length of the first lockout period for a client. It cannot be greater than the maximum value. If you set it to the same value as the maximum, then the lockout period is fixed and does not increase for a client's subsequent lockouts.

- **Range:** 1 through 86400

**Required Privilege Level**

interface

**RELATED DOCUMENTATION**

- *Configuring DHCP Short-Cycle Protection*
- *DHCP Short Cycle Protection Against Frequent Brief or Failed Client Sessions*
single-connection

Syntax

```
single-connection;
```

Hierarchy Level

```
[edit system accounting destination tacplus server server-address]
[edit system tacplus-server server-address],
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 8.5 for SRX Series.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring TACACS+ Authentication | 264
- Configuring TACACS+ System Accounting | 278
sip-server

Syntax

sip-server [address | name];

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information

Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description

Configure Session Initiation Protocol (SIP) server addresses or names for DHCP servers.

Options

address—IPv4 address of the SIP server. To configure multiple SIP servers, include multiple address options. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

name—Fully qualified domain name of the SIP server. To configure multiple SIP servers, include multiple name options. This domain name must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

Required Privilege Level

system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Configuring a DHCP SIP Server (CLI Procedure) | 764 |
| Configuring a DHCP Server on Switches (CLI Procedure) | 759 |
size

Syntax

```plaintext
size bytes;
```

Hierarchy Level

```plaintext
[edit accounting-options file filename]
```

Release Information

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

Description


Options

- `bytes`—Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, `profilelog`) reaches its maximum size, it is renamed `profilelog.0`, then `profilelog.1`, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.

Syntax: x to specify bytes, xk to specify KB, xm to specify MB, xg to specify GB

Range: 256 KB through 1 GB

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring the Maximum Size of the File
List of Syntax
Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches on page 2272
Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600 on page 2272

Syntax: MX, M, T, ACX, PTX Series Routers and EX Series Switches

```
snmp { ... }
```

Syntax: QFX Series Switches, QFabric, OCX1100 and EX4600

```
snmp {
  client-list client-list-name {
    ip-addresses;
  }
  community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
      address restrict;
    }
  }
  logical-system logical-system-name {
    routing-instance routing-instance-name {
      clients {
        addresses;
      }
    }
  }
  routing-instance routing-instance-name {
    clients {
      addresses;
    }
  }
  view view-name;
}
contact contact;
description description;
filter-duplicates;
filter-interfaces;
health-monitor {
  falling-threshold integer;
  interval seconds;
}
```
rising-threshold integer;
}
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}

rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type;
        rising-event-index index;
        rising-threshold integer;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
    }
    history history-index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}

traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regular-expression>;
    flag flag;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance routing-instance-name;
    targets {
        address;
    }
    version (all | v1 | v2);
}

trap-options {
    agent-address outgoing-interface;
    source-address address;
}
v3 {
    notify name {
        tag tag-name;
        type trap;
    }
} notify-filter profile-name {
    oid object-identifier (include | exclude);
}

snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}

target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system logical-system;
    port port-number;
    retry-count number;
    routing-instance routing-instance-name;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
}

target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
        message-processing-model (v1 | v2c | V3);
        security-level (authentication | none | privacy);
        security-model (usm | v1 | v2c);
        security-name security-name;
    }
}

usm {
    local-engine {
        user username {
            authentication-sha {
                authentication-password authentication-password;
            }
            authentication-md5 {
                authentication-password authentication-password;
            }
            authentication-none;
            privacy-aes128 {

privacy-password privacy-password;
}
privacy-des {
    privacy-password privacy-password;
}
privacy-3des {
    privacy-password privacy-password;
}
privacy-none;
}
}
remote-engine engine-id {
    user username {
        authentication-sha {
            authentication-password authentication-password;
        }
        authentication-md5 {
            authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
            privacy-password privacy-password;
        }
        privacy-des {
            privacy-password privacy-password;
        }
        privacy-3des {
            privacy-password privacy-password;
        }
        privacy-none {
            privacy-password privacy-password;
        }
    }
}
}
Hierarchy Level

[edit]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure SNMP.

SNMP modules cannot have the slash (/) character or the @ character in the name.
**Required Privilege Level**

snmp—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- Configuring SNMP on a Device Running Junos OS
- Understanding SNMP Implementation in Junos OS
- Configuring SNMP
source-address (NTP, RADIUS, System Logging, or TACACS+)

Syntax

```
source-address source-address <routing-instance routing-instance-name>;
```

Hierarchy Level

```
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address],
[edit system ntp],
[edit system radius-server server-address],
[edit system syslog],
[edit system tacplus-server server-address]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify a source address for each configured IPv4 or IPv6 TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine.

Options

**source-address**—A valid IP address configured on one of the router or switch interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host hostname** statements at the [edit system syslog] hierarchy level, but not for messages directed to the other Routing Engine.

**routing-instance routing-instance-name**—(Optional) The routing instance name in which the source address is defined.

Default: The primary address of the interface

Required Privilege Level

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

RELATED DOCUMENTATION

| ntp | 2005 |
source-address (SRC Software)

Syntax

source-address source-address;

Hierarchy Level

[edit system services service-deployment]

Release Information

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

Description

Enable Junos OS to work with the Session and Resource Control (SRC) software.

Options

**source-address**— Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.

Required Privilege Level

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

RELATED DOCUMENTATION

| Configuring the Junos OS to Work with SRC Software |
source-address-giaddr

Syntax

source-address-giaddr;

Hierarchy Level

[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface interface-name]

Release Information
Statement introduced in Junos OS Release 10.1 for EX Series switches.

Description
Configure the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent.

When this statement is entered in the [edit forwarding-options helpers bootp] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting all interfaces on the switch.

When this statement is entered in the [edit forwarding-options helpers bootp interface interface-name] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting the specified interface of the switch.

In Junos OS Release 10.1 for EX Series switches and later releases, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is used as the source IP address for relayed DHCP packets by default.

In Junos OS Releases 9.6 and 10.0 for EX Series switches, the gateway IP address of the switch is always used as the source IP address for relayed DHCP packets when the switch is used as the DHCP relay agent.

In Junos OS Releases 9.3 through 9.5 for EX Series switches, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is always used as the source IP address for relayed DHCP packets.

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

RELATED DOCUMENTATION

2281
source-classes

Syntax

```plaintext
source-classes {
    source-class-name;
}
```

Hierarchy Level

```plaintext
[edit accounting-options class-usage-profile profile-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generation FPCs installed.

Description

Specify the source classes for which statistics are collected.

Options

`source-class-name`—Name of the source class to include in the class usage profile.

Required Privilege Level

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

RELATED DOCUMENTATION

`Configuring a Class Usage Profile`
source-ip-change (Forwarding Options)

Syntax

```
source-ip-change;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Release Information
Statement changed from `vpn` to `source-ip-change` in Junos OS Release 15.1X49-D130 and later releases.

Description
For Dynamic Host Configuration Protocol (DHCP) client request forwarding, enable source IP change for the device to use address of egress interface as source IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

- DHCP Overview | 909
ssh (System Services)

Syntax

```bash
ssh {
    authentication-order [method 1 method2 ...];
    ciphers [ cipher-1 cipher-2 cipher-3 ...];
    client-alive-count-max seconds;
    client-alive-interval seconds;
    connection-limit limit;
    fingerprint-hash (md5 | sha2-256);
    hostkey-algorithm (algorithm | no-algorithm);
    key-exchange [algorithm1 algorithm2 ...];
    log-key-changes log-key-changes;
    macs [algorithm1 algorithm2 ...];
    max-pre-authentication-packets number;
    max-sessions-per-connection number;
    no-passwords;
    no-public-keys;
    no-tcp-forwarding;
    protocol-version [v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
    sftp-server;
}
```

tcp-forwarding

Hierarchy Level

[edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
```
client-alive-interval and client-alive-max-count statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.
no-public-keys statement introduced in Junos OS release 15.1.
tcp-forwarding statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.
```
log-key-changes statement introduced in Junos OS Release 17.4R1.
**sftp-server** statement introduced in Junos OS Release 19.1R1.

**Description**
Allow SSH requests from remote systems to access the local router or switch.

The remaining statements are explained separately. Search for a statement in **CLI Explorer** or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**
- Configuring SSH Service for Remote Access to the Router or Switch | 294
ssh-known-hosts

Syntax

```bash
ssh-known-hosts {
  host host-name {
    fetch-from-server host-name;
    load-key-file file-name;
  }
}
```

Hierarchy Level

```
[edit security ssh-known-hosts]
```

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure SSH support for known hosts and for administering SSH host key updates.

Options

host `host-name`—Hostname of the SSH known host entry. This option has the following suboptions:

- **fetch-from-server host-name**—Retrieve SSH public host key information from a specified server.
- **load-key-file filename**—Import SSH host key information from the `/var/tmp/ssh-known-hosts` file.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Security Features on the QFabric System
- Configuring SSH Host Keys for Secure Copying of Data
ssh-known-hosts

Syntax

ssh-known-hosts {
    fetch-from-server server-name;
    host hostname {
        dsa-key dsa-key;
        ecdsa-sha2-nistp256-key ecdsa-sha2-nistp256-key;
        ecdsa-sha2-nistp384-key ecdsa-sha2-nistp384-key;
        ecdsa-sha2-nistp521-key ecdsa-sha2-nistp521-key;
        ed25519-key ed25519-key
        rsa-key rsa-key;
        rsa1-key rsa1-key;
    }
    load-key-file key-file;
}

Hierarchy Level

[edit security]

Release Information

Statement modified in Junos OS Release 8.5.

Description

Configure SSH support for known hosts and for administering SSH host key updates.

Options

- fetch-from-server server-name—Retrieve SSH public host key information from a specified server.
- load-key-file key-file—Import SSH host-key information from the specified /var/tmp/ssh-known-hosts file.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION
ssl-renegotiation

Syntax

ssl-renegotiation;

Hierarchy Level

[edit system services xnm-ssl]

Release Information

Statement introduced in Junos Os Release 13.3.

Description

Enable SSL re-negotiation for xnm-ssl service.

Default

SSL re-negotiation for xnm-ssl service is disabled by default.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
start-time (Accounting)

Syntax

```
start-time time;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information
Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Specify the start time for transfer of an accounting-data log file.

Options

time—Start time for file transfer.

Syntax: `YYYY-MM-DD.hh:mm`

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

RELATED DOCUMENTATION

- Configuring the Start Time for File Transfer
start-time (Authentication Key Transmission)

Syntax

```
start-time (now | yyyy-mm-dd.hh:mm:ss);
```

Hierarchy Level

```
[edit security authentication-key-chains key-chain key-chain-name key key]
```

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.

Options

**now**—Start time as the current year, month, day, hour, minute, and second.

**daydays**—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure `start-time 2day`, the start time will be on the 14th, exactly two days after the configuration is entered.

**hourhours**—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure `start-time 3hour`, the start time will be in 12:00, exactly three hours after the configuration is entered.

**minuteminutes**—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure `start-time 5min`, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.

**monthmonths**—Start time as the specified number of months after the current month. For example, if the current month is March and you configure `start-time 4month`, the start time will be in July, exactly four months after the configuration is entered.
**secondseconds**—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure **start-time 10seconds**, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.

**yearyears**—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure **start-time 1year**, the start time will be in 2012, exactly one year after the configuration is entered.

**yyyy-mm-dd.hh:mm:ss**—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

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

**RELATED DOCUMENTATION**

- Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols
- Example: Configuring BFD Authentication for Securing Static Routes
- Example: Configuring BFD Authentication for Securing Static Routes
- Example: Configuring Hitless Authentication Key Rollover for IS-IS
static (Protocols 802.1X)

Syntax

```
static mac-address {
    interface interface-names;
    vlan-assignment (vlan-id | vlan-name );
}
```

Hierarchy Level

```
[edit protocols dot1x authenticator]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure MAC addresses to exclude from 802.1X authentication. The static MAC list provides an authentication bypass mechanism for supplicants connecting to a port, permitting devices such as printers that are not 802.1X-enabled to be connected to the network on 802.1X-enabled ports.

Using this 802.1X authentication-bypass mechanism, the supplicant connected to the MAC address is assumed to be successfully authenticated and the port is opened for it. No further authentication is done for the supplicant.

You can optionally configure the VLAN that the supplicant is moved to or the interfaces on which the MAC address can gain access from.

Options

- `mac-address` — The MAC address of the device for which 802.1X authentication should be bypassed and the device permitted access to the port.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

```
show dot1x static-mac-address | 2658
```
| Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479 |
| Configuring 802.1X Interface Settings (CLI Procedure) | 390 |

*Configuring 802.1X Authentication (J-Web Procedure)*

| Understanding Authentication on Switches | 361 |
static-binding

**Syntax**

```plaintext
static-binding mac-address {
    client-identifier (ascii client-id | hexadecimal client-id);
    fixed-address {
        address;
    }
    host-name client-hostname;
}
```

**Hierarchy Level**

```
[edit system services dhcp],
[edit system services dhcp]
```

**Release Information**

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

**Description**

For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.

**Options**

- **mac-address**—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.

- **fixed-address address**—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

- **host-name client-hostname**—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the `domain-name` statement.

- **client-identifier (ascii client-id | hexadecimal client-id)**—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

**Required Privilege Level**

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

Syntax

```plaintext
static-subscribers {
    disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Associate subscribers with statically configured interfaces, and provide dynamic service activation for these subscribers.

Options

disable—Disable the static subscribers process.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.
statistics (Access Profile)

Syntax

```
statistics (time | volume-time);
```

Hierarchy Level

```
[edit access profile profile-name accounting]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
`volume-time` option added in Junos OS Release 9.4.

Description

Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.

Options

- `time`—Collect uptime statistics only.
- `volume-time`—Collect both volume and uptime statistics.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Authentication and Accounting Parameters for Subscriber Access
statistics-service

Syntax

```
statistics-service {
    command binary-file-path;
    disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the Packet Forwarding Engine (PFE) statistics service management process.

Options

- **command binary-file-path**—Path to the binary process.
- **disable**—Disable the Packet Forwarding Engine (PFE) statistics service management process.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.
strict (DHCP Local Server)

**Syntax**

strict;

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcpp-local-server dhcppv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcpp-local-server dhcppv6 reconfigure],
[edit logical-systems logical-system-name system services dhcpp-local-server dhcppv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcpp-local-server dhcppv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcpp-local-server dhcppv6 group group-name reconfigure],
[edit system services dhcpp-local-server dhcppv6 reconfigure],
[edit system services dhcpp-local-server dhcppv6 group group-name reconfigure]
```

**Release Information**

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.

**Default**

Accept solicit messages from clients that do not support reconfiguration and permit them to bind.

**Required Privilege Level**

system—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Preventing Binding of Clients That Do Not Support Reconfigure Messages | 789
sub-prefix-length

Syntax

sub-prefix-length sub-prefix-length;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client prefix-delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]

Release Information
Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100. The logical-systems and tenants options are introduced in Junos OS Release 18.4R1.

Description
Allows you to configure DHCPv6 client sub prefix length. The DHCPv6 client separates the delegated prefix according to sub-prefix lengths. If the delegated prefix is not enough for all interfaces, the client sends out a syslog message.

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

RELATED DOCUMENTATION

preferred-prefix-length | 2083
subscriber-management-helper

Syntax

```text
subscriber-management-helper {
    command binary-file-path;
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```text
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the subscriber management helper process.

Options

- **command binary-file-path**—Path to the binary process.
- **disable**—Disable the subscriber management helper process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

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

Syntax

    supplicant (multiple | single | single-secure);

Hierarchy Level

[edit protocols dot1x authenticator interface (all | [interface-names])],
[edit services captive-portal interface (all | interface-names)]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement added to the [edit services captive-portal interface] hierarchy in Junos OS Release 10.1 for EX Series switches
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Configure the MAC-based method used to authenticate clients for 802.1X or captive portal authentication.

Default
single

Options
single—Authenticates only the first client that connects to an authenticator port. All other clients connecting to the authenticator port after the first are permitted free access to the port without further authentication. If the first authenticated client logs out, all other supplicants are locked out until a client authenticates again.

single-secure—Authenticates only one client to connect to an authenticator port. The host must be directly connected to the switch.

multiple—Authenticates multiple clients individually on one authenticator port. You can configure the number of clients per port. If you also configure a maximum number of devices that can be connected to a port through port security settings, the lower of the configured values is used to determine the maximum number of clients allowed per port.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>RELATED DOCUMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch</td>
</tr>
<tr>
<td>Example: Setting Up Captive Portal Authentication on an EX Series Switch</td>
</tr>
<tr>
<td>Understanding Authentication on Switches</td>
</tr>
<tr>
<td>Configuring Captive Portal Authentication (CLI Procedure)</td>
</tr>
</tbody>
</table>
supplicant-timeout

Syntax

supplicant-timeout seconds;

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [interface-name])]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

For 802.1X authentication, configure how long the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.

Default

30 seconds

Options

seconds — Number of seconds.

Range: 1 through 60 seconds
Default: 30 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

| supplicant | 2301 |
| Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440 |
| Understanding Authentication on Switches | 361 |
system-generated-certificate

Syntax

```
system-generated-certificate;
```

Hierarchy Level

```
[edit system services web-management https]
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Configure the automatically generated self-signed certificate for enabling HTTPS services.

Required Privilege Level

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

RELATED DOCUMENTATION

- Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)
tacplus

Syntax

tacplus {
  server {
    server-address {
      port port-number;
      routing-instance routing-instance;
      secret password;
      single-connection;
      timeout seconds;
    }
  }
}

Hierarchy Level

[edit system accounting destination]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
routing-instance option introduced in Junos OS Release 17.4R1.

Description
Configure the Terminal Access Controller Access Control System Plus (TACACS++).

Options
server-address—Address of the TACACS++ authentication server.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring TACACS+ System Accounting | 278
tacplus

Syntax

tacplus {
    server server-address {
        port port-number;
        secret password;
        single-connection;
        source-address source-address;
        timeout seconds;
    }
}

Hierarchy Level

[edit system accounting destination]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure the TACACS+ accounting server.

Options
• server-address —Specify the address of the TACACS+ authentication server.
• port number—Configure the port number on which to contact the TACACS+ server.
• single-connection—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
• source-address address—Configure a source address for each configured TACACS+ server.
• timeout seconds—Configure the amount of time that the local device waits to receive a response from a TACACS+ server.

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

**Syntax**

```plaintext
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    enhanced-accounting;
    strict-authorization
    service-name service-name;
    timestamp-and-timezone;
}
```

**Hierarchy Level**

[edit system]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- `no-cmd-attribute-value` and `exclude-cmd-attribute` options introduced in Junos OS Release 9.3.
- Statement introduced in Junos OS Release 11.1 for QFX Series.
- `timestamp-and-timezone` option introduced in Junos OS Release 12.2.

**Description**

Configure TACACS+ options for authentication and accounting.

**Options**

- `enhanced-accounting`—View the attribute values of a logged in user.

- `exclude-cmd-attribute`—Exclude the `cmd` attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.

- `no-cmd-attribute-value`—Set the `cmd` attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.

- `service-name service-name`—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.

**Default:** junos-exec
**strict-authorization**—Deny login if authorization request fails. When a user is logging in, Junos OS issues two TACACS+ requests—first the authentication request followed by the authorization request. By default, when the authorization request is rejected by the TACACS+ server, Junos OS ignores this and allows full access to the user. When the `set system tacplus-options strict-authorization` statement is set, Junos OS denies access to the user even on failure of the authorization request.

**timestamp-and-timezone**—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>Configuring TACACS+ Authentication</th>
<th>264</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring TACACS+ System Accounting</td>
<td>278</td>
</tr>
<tr>
<td>Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication</td>
<td>218</td>
</tr>
<tr>
<td>enhanced-accounting</td>
<td>1756</td>
</tr>
</tbody>
</table>
TACPLUS-SERVER

Syntax

tacplus-server server-address {
   routing-instance (Accounting and Authentication) routing-instance;
   secret password;
   single-connection;
   source-address source-address;
   timeout seconds;
}

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
routing-instance option introduced in Junos OS Release 17.4R1.

Description

Configure the IPv4 or IPv6 TACACS++ server.

Options

server-address—Address of the IPv4 or IPv6 TACACS++ authentication server.

NOTE: Wildcard characters cannot be used in the TACACS+ server address or source address. This is because the TACACS+ server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

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

Syntax

tacplus-server server-address 
    port port-number;
    secret password;
    single-connection;
    source-address source-address;
    timeoutseconds;
}

Hierarchy Level

[edit system]

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

Description
Configure the TACACS+ server.

Options

- server-address—Address of the TACACS+ authentication server.

    NOTE: Wildcard characters cannot be used in the TACACS server address or source address. This is because the TACACS server and source can accept both IPv4 and IPv6 addresses and, if you use wildcard characters for these addresses, Junos OS cannot validate mismatching server and source address families.

- port—Port number of TACACS+ authentication server.

- secret—Password to use with the RADIUS or TACACS+ server. The secret password used by the local router or switch must match that used by the server. Password to use; can include spaces included in quotation marks.

- single-connection—Optimize attempts to connect to a TACACS+ server. The software maintains one open TCP connection to the server for multiple requests rather than opening a connection for each connection attempt.
• **source-address**—Source address for each configured TACACS+ server, RADIUS server, NTP server, or the source address to record in system log messages that are directed to a remote machine. Configure a valid IP address on one of the device interfaces. For system logging, the address is recorded as the message source in messages sent to the remote machines specified in all **host hostname** statements at the [edit system syslog] hierarchy level.

• **timeout**—The amount of time that the local device waits to receive a response from a RADIUS or TACACS+ server. The timeout range is 1 through 90 seconds. The default is 3 seconds.

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

**RELATED DOCUMENTATION**

Example: Configuring a TACACS+ Server for System Authentication | 268
targets

Syntax

```
targets {
    address;
}
```

Hierarchy Level

```
[edit snmp trap-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure one or more systems to receive SNMP traps.

Options

- `address`—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring SNMP Trap Groups
- Configuring SNMP Trap Groups
tcp-forwarding (JDM)

Syntax

tcp-forwarding;

Hierarchy Level

[edit system services ssh]

Release Information
Statement introduced in Junos OS Release 15.1X53-D50 for the NFX250 Network Services Platform.

Description
Enable a user to create an SSH tunnel over a CLI session to a disaggregated Junos OS platform by using SSH.

Required Privilege Level

RELATED DOCUMENTATION

Configuring SSH Service for Remote Access to the Disaggregated Junos OS Platform
** telnet **

**Syntax**

```
telnet {
    authentication-order [authentication-methods];
    connection-limit limit;
    rate-limit limit;
}
```

**Hierarchy Level**

```
[edit system services]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Provide Telnet connections from remote systems to the local router or switch.

The remaining statements are explained separately. See CLI Explorer.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring Telnet Service for Remote Access to a Router or Switch  |  292
tftp

Syntax

tftp {
    description text-description;
    interface interface-name {
        broadcast;
        description text-description;
        no-listen;
        server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
    }
    server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
}

Hierarchy Level

[edit forwarding-options helpers]

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

Description
Enable TFTP request packet forwarding.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring DNS and TFTP Packet Forwarding
threshold (detection-time)

Syntax

threshold milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd detection-time],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd detection-time],
[edit system services dhcp-local-server group group-name liveness-detection method bfd detection-time],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd detection-time]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the threshold for the adaptation of the detection time. When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

NOTE: The threshold time must be greater than or equal to the minimum-interval or the minimum-receive-interval.

Options

milliseconds—Value for the detection time adaptation threshold.

Range: 1 through 255,000

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

RELATED DOCUMENTATION
threshold (transmit-interval)

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd transmit-interval]
```

Release Information
Statement introduced in Junos OS Release 12.1.

Description
Specify the threshold for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.

Options

```
milliseconds — Threshold value.
```

Range: 0 through 4,294,967,295 ($2^{32} - 1$)

NOTE: The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.

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

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862
timeout (Access Control Service)

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit services unified-access-control]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Configure the amount of time that the switch waits to receive a response from the Junos Pulse Access Control Service.

Options

- `seconds`—Amount of time to wait.

Range: 2 through 1000 seconds

Default: 300 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
timeout (DHCP Local Server)

Syntax

```
timeout timeout-value;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

Options

- `timeout-value`—Initial retry timeout value.

Range: 1 through 10 seconds

Default: 2 seconds
**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients | 847
timeout (System)

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit system radius-server server-address],
[edit system tacplus-server server-address],
[edit system accounting destination radius server server-address],
[edit system accounting destination tacplus server server-address]
```

Release Information

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

Description

Configure the amount of time that the local router or switch waits to receive a response from a RADIUS or TACACS+ server.

Options

- `seconds`—Amount of time to wait.

Range: 1 through 90 seconds

Default: 3 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring RADIUS Server Authentication | 233
- Configuring TACACS+ Authentication | 264
- retry | 2204
**timeout-action (Access Control Service)**

**Syntax**

```plaintext
timeout-action ( close | no-change);
```

**Hierarchy Level**

```
[edit services unified-access-control]
```

**Release Information**

Statement introduced in Junos OS Release 12.2 for EX Series switches.

**Description**

Specify the action to be taken when the timeout is reached for the switch's connection with the Junos Pulse Access Control Service.

**Options**

- **close**—Remove existing sessions and block further traffic.
- **no-change**—Preserve existing connections, but block new sessions.

**Default**: close

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- [timeout (Access Control Service)](#)  | 2321
- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)  | 520
- Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure)  | 523
**tlv-filter**

**Syntax**

```
tlv-filter tlv-name;
```

**Hierarchy Level**

- [edit protocols lldp],
- [edit protocols lldp-med],
- [edit protocols lldp interface interface-name],
- [edit protocols lldp-med interface interface-name]

**Release Information**

Statement introduced in Junos OS Release 18.3 for EX Series switches.

**Description**

Select the type, length, and value (TLV) messages that should not be advertised by Link Layer Discovery Protocol (LLDP) or LLDP Media Endpoint Discovery (LLEP-MED) protocol. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities.

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live.

When you configure the `tlv-filter` statement, you specify the TLVs that you want to disable. This is useful when you want to allow most, but not all, TLVs.

You can also disable TLVs using the `tlv-select` statement. When you configure the tlv-select statement, you specify the TLVs that you want to be advertised by LLDP or LLDP-MED. All other non-mandatory TLVs are disabled.

**NOTE:** The `tlv-select` and `tlv-filter` are mutually exclusive and cannot be used on the same configuration stanza at the same time.

**Default**

All TLVs for LLDP and LLDP-MED are enabled by default.

**Options**
The following options can be configured using `tlv-filter` at the `[edit protocols lldp]` and `[edit protocols lldp interface interface-name]` hierarchy levels:

**port-description**—The user-configured port description.

**system-name**—The user-configured name of the local system.

**system-description**—The user-configured name of the local system.

**system-capabilities**—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.

**management-address**—IP management address of the local system.

**mac-phy-config-status**—Advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type.

**power-vi-mdi**—Advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.

**link-aggregation**—Advertises whether the port is aggregated and its aggregated port ID.

**maximum-frame-size**—The maximum transmission unit (MTU) of the interface sending LLDP frames.

**jnpr-chassis-serial**—The chassis serial number.

**jnpr-vcp**—Juniper virtual chassis port.

**port-vid**—Indicates the port VLAN ID that will be associated with an untagged or priority tagged data frame received on the VLAN port.

**vlan-name**—Indicates the assigned name of any VLAN at the device.

The following options can be configured using `tlv-filter` at the `[edit protocols lldp-med]` and `[edit protocols lldp-med interface interface-name]` hierarchy levels:

**ext-power-via-mdi**—The power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

**location-id**—The physical location of the endpoint.

**med-capabilities**—The primary function of the port.

**network-policy**—The port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

RELATED DOCUMENTATION
- show lldp | 2680
- Configuring LLDP (CLI Procedure) | 654
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
**tlv-select**

**Syntax**

```
tlv-select tlv-name;
```

**Hierarchy Level**

```
[edit protocols lldp],
[edit protocols lldp-med],
[edit protocols lldp interface interface-name],
[edit protocols lldp-med interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 18.3 for EX Series switches.

**Description**

Select the type, length, and value (TLV) messages that should be advertised by Link Layer Discovery Protocol (LLDP) or LLDP Media Endpoint Discovery (LLEP-MED) protocol. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities.

In multi-vendor networks, it might not be desirable to send TLV messages because they can contain sensitive information about a network device. You can configure LLDP or LLDP-MED to disable any non-mandatory TLV message. Mandatory TLVs are: chassis-id, port-id, and time-to-live.

When you configure the tlv-select statement, you specify the TLVs that should be advertised by LLDP or LLDP-MED. All other non-mandatory TLVs are disabled. This is useful when you want to disable most, but not all, TLVs.

You can also disable TLVs using the tlv-filter statement. When you configure the tlv-filter statement, you specify the TLVs that should be disabled.

**NOTE:** The tlv-select and tlv-filter are mutually exclusive and cannot be used on the same configuration stanza at the same time.

**Default**

All TLVs for LLDP and LLDP-MED are enabled by default.

**Options**
The following options can be configured using `tlv-select` at the [edit protocols lldp] and [edit protocols lldp interface interface-name] hierarchy levels:

**port-description**—The user-configured port description.

**system-name**—The user-configured name of the local system.

**system-description**—The user-configured name of the local system.

**system-capabilities**—The primary function performed by the system. The capabilities that system supports are defined; for example, bridge or router. This information cannot be configured, but is based on the model of the product.

**management-address**—IP management address of the local system.

**mac-phy-config-status**—Advertises information about the physical interface, such as autonegotiation status and support and MAU (medium attachment unit) type.

**power-vi-mdi**—Advertises MDI (media dependent interface) power support, PSE (power sourcing equipment) power pair, and power class information.

**link-aggregation**—Advertises whether the port is aggregated and its aggregated port ID.

**maximum-frame-size**—The maximum transmission unit (MTU) of the interface sending LLDP frames.

**jnpr-chassis-serial**—The chassis serial number.

**jnpr-vcp**—Juniper virtual chassis port.

**port-vid**—Indicates the port VLAN ID that will be associated with an untagged or priority tagged data frame received on the VLAN port.

**vlan-name**—Indicates the assigned name of any VLAN at the device.

The following options can be configured using `tlv-select` at the [edit protocols lldp-med] and [edit protocols lldp-med interface interface-name] hierarchy levels:

**ext-power-via-mdi**—The power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

**location-id**—The physical location of the endpoint.

**med-capabilities**—The primary function of the port.

**network-policy**—The port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.
Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

RELATED DOCUMENTATION

| show lldp | 2680 |
| Configuring LLDP (CLI Procedure) | 654 |
| Understanding LLDP and LLDP-MED on EX Series Switches | 661 |
**token (DHCP Local Server)**

**Syntax**

```
token token-value;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

**Description**

Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, *Authentication for DHCP Messages*, section 4.

**Options**
**token-value**—Plain-text alphanumeric string.

**Default:** null (empty string)

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

**RELATED DOCUMENTATION**

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Configuring a Token for DHCP Local Server Authentication | 782
trace (DHCP Relay Agent)

Syntax

```
trace;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 10.4.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Enable trace operations for a group of interfaces or for a specific interface within a group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) | 783
- Tracing Extended DHCP Operations
Tracing Extended DHCP Operations for Specific Interfaces
traceoptions (802.1X)

Syntax

```plaintext
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
    flag flag;
}
```

Hierarchy Level

```
[edit protocols dot1x]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `dot1x-event` and `dot1x-ipc` options introduced in Junos OS Release 13.2X50 for EX Series switches.

Description

Define tracing operations for the 802.1X protocol.

Default

Tracing operations are disabled.

Options

- **file filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size by using the `size` option.

  Range: 2 through 1000

  Default: 3 files

- **flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

  - **all**—All tracing operations.
  - **config-internal**—Trace internal configuration operations.
  - **dot1x-event**—(Switches with ELS only) Trace 802.1x events.
  - **dot1x-debug**—(Switches without ELS) Trace 802.1x events.
- **dot1x-ipc**—(Switches with ELS only) Trace IPC interactions.
- **eapol**—Trace EAPOL packets transmitted and received.
- **esw-if**—(Switches without ELS) Trace ESW interactions.
- **general**—Trace general operations.
- **normal**—Trace normal operations.
- **parse**—Trace reading of the configuration.
- **regex-parse**—Trace regular-expression parsing operations.
- **state**—Trace protocol state changes.
- **task**—Trace protocol task operations.
- **timer**—Trace protocol timer operations.
- **vlan**—Trace VLAN transactions.

**match regex**—(Optional) Refine the output to include lines that contain the regular expression.

**no-world-readable**—(Optional) Restrict file access to the user who created the file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files with the files option, you also must specify a maximum file size.

Syntax: \texttt{xk} to specify KB, \texttt{xm} to specify MB, or \texttt{xg} to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- show lldp  | 2680
- Configuring 802.1X Interface Settings (CLI Procedure)  | 390
- 802.1X for Switches Overview  | 387
traceoptions (Address-Assignment Pool)

Syntax

```
traceoptions {
    file filename {
        files number;
        size maximum-file-size;
        match regex;
        (world-readable | no-world-readable);
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}
```

Hierarchy Level

```
[edit system processes general-authentication-service]
```

Release Information
Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.

Option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure tracing options.

Options

**file** `filename`—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory `/var/log`.

**files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the `size` option and a filename.

**Range:** 2 through 1000
Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- address-assignment—All address-assignment events
- all—All tracing operations
- configuration—Configuration events
- framework—Authentication framework events
- ldap—LDAP authentication events
- local-authentication—Local authentication events
- radius—RADIUS authentication events

match regex—(Optional) Refine the output to include lines that contain the regular expression.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: xk to specify KB, xm to specify MB, or xg to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

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

RELATED DOCUMENTATION

Address-Assignment Pool Configuration Overview
traceoptions (DHCP)

Syntax

```plaintext
traceoptions {
  file filename <files number> <match regular-expression> <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level

[edit system processes dhcp-service]
[edit security dynamic-address]

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 18.4R1.

Description

Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.

This statement replaces the deprecated `traceoptions` statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.

**NOTE:** Traceoptions does not differentiate between a logical system and tenant system, and can be configured under the root logical system.

Options

- **file filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

- **files number**—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

  **Range:** 2 through 1000

  **Default:** 3 files
flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:

- **all**—Trace all events.
- **auth**—Trace authentication events.
- **database**—Trace database events.
- **fwd**—Trace firewall process events.
- **general**—Trace miscellaneous events.
- **ha**—Trace high availability-related events.
- **interface**—Trace interface operations.
- **io**—Trace I/O operations.
- **liveness-detection**—Trace liveness detection operations.
- **packet**—Trace packet and option decoding operations.
- **performance**—Trace performance measurement operations.
- **profile**—Trace profile operations.
- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **security-persistence**—Trace security persistence events.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.
level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

**Default:** error

**match regular-expression**—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access, allowing only the user root and users who have the Junos OS maintenance permission to access the trace files.

**size maximum-file-size**—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (**maximum-file-size**k), megabytes (**maximum-file-size**m), or gigabytes (**maximum-file-size**g). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Range:** 10,240 through 1,073,741,824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**

trace—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

| Tracing Extended DHCP Operations |
traceoptions (DHCP Server)

Syntax

```
traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

```
[edit system services dhcp]
```

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

Description
Define tracing operations for DHCP processes.

Options

- **file filename**—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory /var/log.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the `size` option and a filename.

  **Range:** 2 through 1000

  **Default:** 3 files

- **flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:

  - **all**—All tracing operations
  - **binding**—Trace binding operations
  - **config**—Log reading of configuration
  - **conflict**—Trace user-detected conflicts for IP addresses
  - **event**—Trace important events
  - **ifdb**—Trace interface database operations
• **io**—Trace I/O operations
• **lease**—Trace lease operations
• **main**—Trace main loop operations
• **misc**—Trace miscellaneous operations
• **packet**—Trace DHCP packets
• **options**—Trace DHCP options
• **pool**—Trace address pool operations
• **protocol**—Trace protocol operations
• **rtsock**—Trace routing socket operations
• **scope**—Trace scope operations
• **signal**—Trace DHCP signal operations
• **trace**—All tracing operations
• **ui**—Trace user interface operations

**match regex**—(Optional) Refine the output to include lines that contain the regular expression.
- all—All tracing operations
- binding—Trace binding operations
- config—Log reading of configuration
- conflict—Trace user-detected conflicts for IP addresses
- event—Trace important events
- ifdb—Trace interface database operations
- io—Trace I/O operations
- lease—Trace lease operations
- main—Trace main loop operations
- match regex—Refine the output to include lines that contain the regular expression.
- misc—Trace miscellaneous operations
- packet—Trace DHCP packets
- options—Trace DHCP options
- pool—Trace address pool operations
- protocol—Trace protocol operations
- rtsock—Trace routing socket operations
- scope—Trace scope operations
- signal—Trace DHCP signal operations
- trace—All tracing operations
- ui—Trace user interface operations

no-world-readable—(Optional) Disable unrestricted file access.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named \textit{trace-file} reaches this size, it is renamed \textit{trace-file.0}. When the \textit{trace-file} again reaches its maximum size, \textit{trace-file.0} is renamed \textit{trace-file.1} and \textit{trace-file} is renamed \textit{trace-file.0}. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the \texttt{files} option and filename.

\textbf{Syntax:} \texttt{xk} to specify KB, \texttt{xm} to specify MB, or \texttt{xg} to specify GB

\textbf{Range:} 10 KB through 1 GB

\textbf{Default:} 128 KB

world-readable—(Optional) Enable unrestricted file access.
Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Tracing Operations for DHCP Processes | 713
System Management Configuration Statements
traceoptions (DNS, Port, and TFTP Packet Forwarding)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size bytes> <world-readable | no-world-readable>;
    flag flag;
    level level;
    <no-remote-trace>;
}
```

Hierarchy Level

[edit forwarding-options helpers]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement standardized and match option introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure tracing operations for BOOTP, DNS, TFTP, or custom UDP port packet forwarding.

Default

If you do not include this statement, no tracing operations are performed.

Options

- **file filename**—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named `fud` in the directory `/var/log`. If you include the `file` statement, you must specify a filename.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the `size` option and a filename.

  **Range:** 2 through 1000

  **Default:** 3 files

- **flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:
• **address**—Trace address management events
• **all**—Trace all events
• **bootp**—Trace BOOTP or DHCP services events
• **config**—Trace configuration events
• **domain**—Trace DNS service events
• **ifdb**—Trace interface database operations
• **io**—Trace I/O operations
• **main**—Trace main loop events
• **port**—Trace arbitrary protocol events
• **rtsock**—Trace routing socket operations
• **tftp**—Trace TFTP service events
• **trace**—Trace tracing operations
• **ui**—Trace user interface operations
• **util**—Trace miscellaneous utility operations

**match regular-expression**—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—(Optional) Disable remote tracing globally or for a specific tracing operation.

**no-world-readable**—(Optional) Restrict file access to the owner.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the `trace-file` file again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option and filename.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 0 bytes through 4,294,967,295 KB

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
RELATED DOCUMENTATION

Tracing BOOTP, DNS, and TFTP Forwarding Operations
traceoptions (LLDP)

Syntax

```
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag <disable>;
}
```

Hierarchy Level

```
[edit protocols lldp],
[edit routing-instances routing-instance-name protocols lldp]
```

Release Information


Description

Set LLDP protocol-level tracing options.

Default

The default LLDP protocol-level trace options are inherited from the global `traceoptions` statement.

Options

disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place spanning-tree protocol tracing output in the file `/var/log/stp-log`.

files number—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files

Default: 1 trace file only

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the LLDP-specific tracing options:

- all—Trace all operations.
- config—Log configuration events.
- **interface**—Trace interface update events.
- **protocol**—Trace protocol information.
- **rtsock**—Trace socket events.
- **vlan**—Trace vlan update events.

The following are the global tracing options:
- **all**—All tracing operations.
- **config-internal**—Trace configuration internals.
- **general**—Trace general events.
- **normal**—All normal events. This is the default. If you do not specify this option, only unusual or abnormal operations are traced.
- **parse**—Trace configuration parsing.
- **policy**—Trace policy operations and actions.
- **regex-parse**—Trace regular-expression parsing.
- **route**—Trace routing table changes.
- **state**—Trace state transitions.
- **task**—Trace protocol task processing.
- **timer**—Trace protocol task timer processing.

**no-world-readable**—(Optional) Prevent any user from reading the log file. This is the default. If you do not include this option, tracing output is appended to an existing trace file.

**size maximum-file-size**—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the `trace-file` again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also specify a maximum number of trace files with the files option.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 1 MB

**world-readable**—(Optional) Allow any user to read the log file.
Required Privilege Level

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

RELATED DOCUMENTATION

Tracing LLDP Operations
traceoptions (LLDP)

Syntax

```
traceoptions {
    file filename <files number> <size size> <world-readable|no-world-readable> <no-stamp> <replace>;
    flag flag <disable>;
}
```

Hierarchy Level

```
[edit protocols lldp]
```

Release Information

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

Description

Define tracing operations for the Link Layer Discovery Protocol (LLDP). You can trace messages under LLDP for LLDP and PTOPO MIBs.

NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

Default

Tracing operations are disabled.

Options

- **file filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

  Range: 2 through 1000

  Default: 3 files
flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—All tracing operations.
- configuration—Trace configuration operations.
- interface—Trace interface update events.
- netbios—Trace NetBIOS events.
- packet—Trace packet events.
- rtsock—Trace routing socket operations.
- snmp—Trace SNMP configuration operations.
- vlan—Trace VLAN update events.

no-stamp—(Optional) Do not timestamp the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Restrict file access to the user who created the file.

replace—(Optional) Replace an existing trace file if there is one rather than appending output to it.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the files option.

Syntax: xk to specify KB, xn to specify MB, or xg to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

Default: If you do not include this option, tracing output is appended to an existing trace file.

world-readable—(Optional) Enable unrestricted file access.

NOTE: The traceoptions statement is not supported on the QFX3000 QFabric system.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.
<table>
<thead>
<tr>
<th>RELATED DOCUMENTATION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring LLDP-MED (CLI Procedure)</td>
<td>665</td>
</tr>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
<td>661</td>
</tr>
<tr>
<td>Understanding LLDP</td>
<td>653</td>
</tr>
</tbody>
</table>
traceoptions (Outbound SSH)

Syntax

```
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
}
```

Hierarchy Level

[edit system services outbound-ssh]

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Set the trace options.

Options

- **file**—Configure the trace file information.
  - **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, the name of the file is the name of the process being traced.
  - **files number**—Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed to `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

    Range: 2 through 1000 files

    Default: 10 files
  
  - **match regular-expression**—Refine the output to include lines that contain the regular expression.
size maximum-file-size—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renamings scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Syntax: x K to specify KB, x m to specify MB, or x g to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable | no-world-readable—By default, log files can be accessed only by the user who configures the tracing operation. The world-readable option enables any user to read the file. To explicitly set the default behavior, use the no-world-readable option.

flag—Specify the tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.

• all—Trace all events.

• configuration—Trace configuration events.

• connectivity—Trace TCP connection handling.

no-remote-trace—Disable remote tracing.

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

RELATED DOCUMENTATION

Displaying Log and Trace Files
traceoptions (SBC Configuration Process)

Syntax

```
traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

```
[edit system processes sbc-configuration-process]
```

Release Information
Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description
Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG).

Options
- **file filename**—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory `/var/log`. You can include the following file options:
  - **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
    - If you specify a maximum number of files, you must also specify a maximum file size with the `size` option and a filename.
  - **match regex**—(Optional) Refine the output to include lines that contain the regular expression.
  - **no-world-readable**—(Optional) Disable unrestricted file access.
  - **size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the trace-file again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest
trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number
of trace files with the files option and filename.

Syntax: \texttt{xk} to specify KB, \texttt{xm} to specify MB, or \texttt{xg} to specify GB.
Range: 10 KB through 1 GB
Default: 128 KB

- \texttt{world-readable} (Optional) Enable unrestricted file access.

\textbf{flag flag}—Tracing operation to perform. To specify more than one tracing operation, include multiple \texttt{flag} statements. You can include the following flags:

- \texttt{all trace-level}—Trace all SBC process operations.
- \texttt{common trace-level}—Trace common events.
- \texttt{configuration trace-level}—Trace configuration events.
- \texttt{device-monitor trace-level}—Trace device monitor events.
- \texttt{ipc trace-level}—Trace IPC events.
- \texttt{memory—pool trace-level}—Trace memory pool events.
- \texttt{trace-level}—Trace level options are related to the severity of the event being traced. When you choose
  a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels
  as the \texttt{trace-level}:
  - \texttt{debug}—Log all code flow of control.
  - \texttt{error}—Log failures with a short-term effect.
  - \texttt{info}—Log summary for normal operations, such as the policy decisions made for a call.
  - \texttt{trace}—Log program trace START and EXIT macros.
  - \texttt{warning}—Log failure recovery events or failure of an external entity.
- \texttt{ui trace-level}—Trace user interface operations.

\textbf{Required Privilege Level}

\texttt{system}—To view this statement in the configuration.
\texttt{system-control}—To add this statement to the configuration.

\textbf{RELATED DOCUMENTATION}

See "Troubleshooting the IMSG" in the \textit{Junos Multiplay Solutions Guide}
\textit{System Management Configuration Statements}
traceoptions (Security)

Syntax

traceoptions {
    file filename <files number> <size size>
    flag all;
    flag certificates;
    flag database;
    flag general;
    flag ike;
    flag parse;
    flag policy-manager;
    flag routing-socket;
    flag timer;
    level
    no-remote-trace
}

Hierarchy Level

[edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure security trace options.

To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the /var/log/kmd file.

NOTE: The traceoptions statement is not supported on QFabric systems.
Options

files number—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files
Default: 0 files

size size—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, kmd) reaches this size, it is renamed, kmd.0, then kmd.1 and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

flag flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- all—Trace all security events.
- certificates—Trace certificate events.
- database—Trace database events.
- general—Trace general events.
- ike—Trace IKE module processing.
- parse—Trace configuration processing.
- policy-manager—Trace policy manager processing.
- routing-socket—Trace routing socket messages.
- timer—Trace internal timer events.

level level—(Optional) Set trace options level.

- all—match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match conditions that should be handled specially.
- verbose—Match verbose messages.
- warning—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing
Required Privilege Level
admin—To view the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Tracing Operations
transfer-interval

Syntax

```
transfer-interval minutes;
```

Hierarchy Level

```
[edit accounting-options file filename]
```

Release Information

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

Description

Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.

Options

```
minutes — Time the file remains open and receives new statistics before it is closed and transferred to an archive site.
```

Range: 5 through 2880 minutes
Default: 30 minutes

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Transfer Interval of the File
transmit-delay (LLDP)

**Syntax**

transmit-delay seconds;

**Hierarchy Level**

- [edit protocols lldp],
- [edit routing-instances routing-instance-name protocols lldp]

**Release Information**


**Description**

(MX Series and T Series routers only) Configure a delay between two successive LLDP advertisements.

**Options**

- **seconds**—Delay between two successive LLDP advertisements.

**Default:** 2

**Range:** 1 through 8192

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring LLDP
transmit-delay

Syntax

transmit-delay seconds;

Hierarchy Level

[edit protocols lldp]

Release Information

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

Description

Specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in the Link Layer Discovery Protocol (LLDP) or in the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system.

The advertisement-interval value must be greater than or equal to four times the transmit-delay value, or an error will be returned when you attempt to commit the configuration.

Default

Enabled

Options

seconds—Delay after a change to the local TLVs or system state before LLDP advertisements are sent.

Range: 1 through 8192 seconds

Default:

• 2 seconds if the advertisement-interval value is set to 8 seconds or more
• 1 second if the advertisement-interval value is set to less than 8 seconds

Required Privilege Level

routing—To view this statement in the configuration.

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

RELATED DOCUMENTATION

show lldp | 2680
<table>
<thead>
<tr>
<th>Configuring LLDP (CLI Procedure)</th>
<th>654</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
<td>661</td>
</tr>
</tbody>
</table>
transmit-interval

Syntax

```conf
transmit-interval {
    threshold milliseconds;
    minimum-interval milliseconds;
}
```

Hierarchy Level

- [edit system services dhcp-local-server liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
- [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
- [edit system services dhcp-local-server group group-name liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the Bidirectional Forwarding Detection (BFD) transmit interval.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

Related Documentation

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients
transmit-period

Syntax

transmit-period seconds;

Hierarchy Level

[edit protocols dot1x authenticator interface (802.1X) (all | [interface-name])]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
For 802.1X authentication, how long the port waits before retransmitting the initial EAPOL PDUs to the supplicant.

Default
30 seconds

Options
seconds—Number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant.

Range: 1 through 65,535 seconds
Default: 30 seconds

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

RELATED DOCUMENTATION

Configuring 802.1X Interface Settings (CLI Procedure) | 390
802.1X for Switches Overview | 387
trap-group

List of Syntax
Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls on page 2369
Syntax: QFX and EX Series Switches and OCX1100 on page 2369

Syntax: MX, M, T, ACX and PTX Series routers, OCX1100, EX and QFX Series Switches and SRX and vSRX firewalls

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    routing-instance instance;
    targets {
        address;
    }
    version (all | v1 | v2);
}
```

Syntax: QFX and EX Series Switches and OCX1100

```
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    targets {
        address;
    }
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, and SRX and vSRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

**Options**
- **group-name**—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately. See CLI Explorer.

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

**RELATED DOCUMENTATION**

- Configuring SNMP Trap Groups
- Configuring SNMP Trap Groups
trap-options

List of Syntax
Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls on page 2371
QFX Series Switches, EX4600, OCX1100 on page 2371

Syntax: MX, M, T, ACX and PTX Series Routers, EX Series Switches and SRX Firewalls

```
trap-options {
  agent-address outgoing-interface;
  context-oid;
  enterprise-oid;
  logical-system logical-system-name {
    routing-instance routing-instance-name {
      source-address address;
    }
  }
  routing-instance routing-instance-name {
    source-address address;
  }
}
```

QFX Series Switches, EX4600, OCX1100

```
trap-options {
  agent-address outgoing-interface;
  source-address address;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series Routers, and SRX Firewalls.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
context-oid option introduced in Junos OS Release 17.1.

Description
Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.

Default
Disabled

Options

context-oid—Add context oid in varbind of all traps originating from non-default logical system and routing instance. If your network management system is not able to handle prefixes such as `<routing-instance name>@<trap-group-name>` or `<logical-system name>/<routing-instance name>@<trap-group-name>`, setting the context-oid configuration statement will send only the `<trap-group-name>` and add `<logical-system name>/<routing-instance name>` as an additional varbind.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring SNMP Trap Options
trigger (DHCP Local Server)

Syntax

```
trigger {
    radius-disconnect;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
**Required Privilege Level**

*system*—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

- Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | 848
- radius-disconnect | 2139
tries-before-disconnect

Syntax

tries-before-disconnect number;

Hierarchy Level

[edit system login retry-options]

Release Information

Statement introduced in Junos OS Release 8.0.

Description

Configure the maximum number of times the user is allowed to enter a password to attempt to log in to the router through SSH or Telnet.

Options

number—Maximum number of times a user is allowed to attempt to enter a password to log in through SSH or Telnet.

Range: 1 through 10

Default: 10

Required Privilege Level

admin—To view this statement in the configuration.

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

RELATED DOCUMENTATION

| Limiting the Number of User Login Attempts for SSH and Telnet Sessions | 82 |
| retry-options | 2205 |
trust-option-82

Syntax

trust-option-82;

Hierarchy Level

[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.

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

RELATED DOCUMENTATION

| Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | 822 |
| Overriding the Default DHCP Relay Configuration Settings | 803 |
trusted-key

Syntax

trusted-key [key-numbers];

Hierarchy Level

[edit system ntp]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For NTP, configure the keys you are allowed to use when you configure the SRX Series device to synchronize its time with other systems on the network.

Options

key-numbers—One or more key numbers. Each key can be any 32-bit unsigned integer except 0.

Required Privilege Level

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

RELATED DOCUMENTATION

ntp | 2005
uac-policy

Syntax

uac-policy;

Hierarchy Level

[edit ethernet-switching-options]

Release Information
Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description
Configure Junos Pulse Access Control Service as the access policy to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.

Default
The Access Control Service access policy is disabled.

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

RELATED DOCUMENTATION

| Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520 |
| Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523 |
uac-service

Syntax

```bash
uac-service {
  timeout {
    timeout-action {
      Hierarchy Level

      [edit system processes]

      Release Information
      Statement introduced in Junos OS Release 12.2 for EX Series switches.

      Description
      Configure Junos Pulse Access Control Service as one of the system processes.

      Default
      Junos Pulse Access Control Service process is disabled.

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

      RELATED DOCUMENTATION
      Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520
      Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523
      Understanding Centralized Network Access Control and EX Series Switches | 517
```
**uac-service**

**Syntax**

```plaintext
uac-service {
  command binary-file-path;
  disable;
  failover (alternate-media | other-routing-engine);
}
```

**Hierarchy Level**

```
[edit system processes]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.

**Description**

Specify the unified access control daemon process.

**Options**

- **command binary-file-path**—Path to the binary process.
- **disable**—Disable the unified access control daemon process.
- **failover**—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - **alternate-media**—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - **other-routing-engine**—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Firewall User Authentication Overview*
unattended-boot

Syntax

unattended-boot;

Hierarchy Level

[edit system]

Release Information
Statement introduced in Junos OS Release 13.2X51-D20 for EX Series switches.

Description
Set the switch to unattended mode for U-Boot to prevent unauthorized access to the system before the JUNOS OS login prompt appears. In unattended mode, access to the loader CLI is blocked, as well as recovery mechanisms such as password recovery by using single-user mode and booting the switch by using a USB flash drive. In order to access the CLI in U-Boot mode, the user must enter a boot-loader password that has been previously configured.

NOTE: If the root password is lost while the switch is in unattended mode, the switch must be reset to the factory default configuration using the LCD panel. For more information see Reverting to the Default Factory Configuration for the EX Series Switch.

Default
Unattended mode is not enabled by default.

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

RELATED DOCUMENTATION

Using Unattended Mode for U-Boot to Prevent Unauthorized Access | 375
boot-loader-authentication | 1538
unified-access-control

Syntax

unified-access-control {
  infranet-controller {
    hostname {
      address ip-address;
      interface interface-name;
      password password;
      port port-number;
    }
  }
}

Hierarchy Level

[edit services]

Release Information
Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description
Configure Junos Pulse Access Control Service to authenticate and authorize users connected to the switch for admission to the network and for access to protected network resources.

The remaining statements are explained separately. See CLI Explorer.

Default
Junos Pulse Access Control Service is disabled.

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

RELATED DOCUMENTATION

| Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure) | 520 |
| Configuring the EX Series Switch for Captive Portal Authentication with Junos Pulse Access Control Service (CLI Procedure) | 523 |
update-interval

Syntax

update-interval minutes;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

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

Description

Enable interim accounting updates and configure the amount of time that the router or switch waits before sending a new accounting update.

Interim accounting updates are included in the exchange of messages between the client and the accounting server. In RADIUS accounting, the client is the network access server (NAS), which can be the router or switch. The NAS sends Accounting-Request messages to the server, which acknowledges receipt of the requests with Accounting-Response messages. Interim accounting updates are sent in Accounting-Request packets with the Acct-Status-Type attribute set to Interim-Update.

When a user is authenticated, the authentication server issues an Access-Accept message in response to a successful Access-Request message. The interval between interim updates can be configured directly on the server using the Acct-Interim-Interval attribute of the Access-Accept message. However, if the update interval is configured on the NAS using update-interval, then the locally configured value overrides the value found in an Access-Accept message from the server.

NOTE: All information in an interim update message is cumulative from the beginning of the session, not from the last interim update message.

Default

No interim updates are sent from the client to the accounting server.

Options

minutes—Amount of time between updates, in minutes. All values are rounded to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.

Range: 10 through 1440 minutes
Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications
update-router-advertisement

Syntax

update-router-advertisement (interface interface-name);

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]

Release Information
Statement introduced in Junos OS Release 12.1X45-D10.
The logical-systems and tenant options are introduced in Junos OS Release 18.4R1.

Description
Specify the interface used to delegate prefixes.

Options
interface interface-name—Interface on which to delegate prefixes

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

RELATED DOCUMENTATION
**update-server**

**Syntax**

```plaintext
update-server;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

**Release Information**

Statement introduced in Junos OS Release 8.5 for J Series devices.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch, router, or device.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- **Configuring a DHCP Client (CLI Procedure)** | 762
- **Example: Configuring the Device as a DHCP Client** | 937

```
interfaces
unit
family
```
**update-server (dhcp-client)**

**Syntax**

```
update-server;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

**Release Information**

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

**Description**

Propagate DHCP options to a local DHCP server.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**
update-server (dhcpv6-client)

Syntax

update-server;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

Description
Propagate TCP/IP settings to the DHCPv6 server.

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

RELATED DOCUMENTATION
usb-control

Syntax

```
usb-control {
    command binary-file-path;
    disable;
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description

Specify the universal serial bus (USB) supervise process.

Options

- **command binary-file-path**—Path to the binary process.
- **disable**—Disable the universal serial bus (USB) supervise process.

Required Privilege Level

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

Syntax

use-interface-description {logical | device};

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-identifier]

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description

The description configured at the physical or logical interface level is used for client identification.

Required Privilege Level

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

RELATED DOCUMENTATION
use-interface-description

Syntax

use-interface-description (logical | device);

Hierarchy Level

[edit forwarding-options dhcp dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp relay relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp relay relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]

Release Information

Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.
Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.
Support at the [edit vlans vlan-name dhcp-security dhcpv6-options option-18] and [edit vlans vlan-name dhcp-security dhcpv6-options option-37] hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description

Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.

NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID.
You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

The textual description is configured using the `description` statement at the `[edit interfaces interface-name]` hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name. When you use the interface description rather than the interface name, the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used. To include the IRB interface description instead of the Layer 2 interface description, configure the `use-interface-description` and the `no-vlan-interface-name` statements. If no description is configured for the IRB interface, DHCP relay defaults to using the IRB interface name.

**NOTE:** The `use-interface-description` statement is mutually exclusive with the `use-vlan-id` statement.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.

**NOTE:** By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

**Options**

- **logical**—Use the textual description that is configured for the logical interface.
- **device**—Use the textual description that is configured for the device interface.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.
RELATED DOCUMENTATION

Including a Textual Description in DHCP Options

Using DHCP Relay Agent Option 82 Information | 739

Configuring DHCPv6 Relay Agent Options
use-primary (DHCP Local Server)

Syntax

```bash
use-primary primary-profile-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server
group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server dynamic-profile profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name dynamic-profile
profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server dynamic-profile profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name dynamic-profile
profile-name],
[edit system services dhcp-local-server dynamic-profile profile-name],
[edit system services dhcp-local-server group group-name dynamic-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber or DHCP client logs in. Subsequent subscribers (or clients) are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber (or client) logs out, the next subscriber (or client) that logs in is assigned the primary dynamic profile.

Options

`primary-profile-name`—Name of the dynamic profile to configure as the primary dynamic profile

Required Privilege Level

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

RELATED DOCUMENTATION
Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
use-primary (DHCP Relay Agent)

Syntax

```
use-primary primary-profile-name;
```

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name dynamic-profile profile-name],
[edit forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name]

Release Information

Statement introduced in Junos OS Release 9.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

Description
Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

**Options**

*primary-profile-name*—Name of the dynamic profile to configure as the primary dynamic profile

**Required Privilege Level**

system—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

*Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
use-vlan-id

Syntax

use-vlan-id;

For Platforms with Enhanced Layer 2 Software (ELS)

[edit forwarding-options helpers bootp dhcp-option82-circuit-id]
[edit forwarding-options helpers bootp interface interface-name dhcp-option82-circuit-id]

For MX Series Platforms

[edit bridge-domains bridge-domain-name forwarding-options dhcp-security option-82 circuit-id]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

NOTE: The EX Series switches that support the use-vlan-id statement are the EX4300, EX4600, and EX9200 switches.

Description

Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.

NOTE: The use-vlan-id statement is mutually exclusive with the use-interface-description and no-vlan-interface-name statements.

The use-vlan-id statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

(fe | ge)-fpc/pic/port.subunit:svlan_id-vlan_id
NOTE: The subunit is required and used to differentiate the interface for remote systems, and svlan_id-vlan_id represents the VLANs associated with the bridge domain.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Example: Setting Up DHCP Option 82 Using the Same VLAN*
- *Example: Setting Up DHCP Option 82*
use-vlan-id (DHCP Relay Agent)

Syntax

use-vlan-id;

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group ]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Specify that the VLAN is identified by the VLAN ID, rather than the VLAN name, when you configure the DHCPv6 relay agent to include either of the following in packets it sends to a DHCPv6 server:

- DHCPv6 Interface-ID (option 18)
- DHCPv6 Remote-ID (option 37)

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

RELATED DOCUMENTATION

Configuring DHCPv6 Relay Agent Options
user (Access)

Syntax

```plaintext
user user-name {
  authentication {
    encrypted-password encrypted-password;
    no-public-keys;
    ssh-ecdsa name {
      from host-list;
    }
    ssh-ed25519 name {
      from host-list;
    }
    ssh-rsa name {
      from host-list;
    }
  }
  class class-name;
  cli {
    prompt prompt;
  }
  full-name complete-name;
  uid uid;
}
```

Hierarchy Level

```plaintext
[edit system login]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement **no-public-keys** introduced in Junos OS Release 15.1.
Statement **cli** introduced in Junos OS 17.3.

Description

Configure access permission for individual users. Starting in Junos OS Release 18.3, the **ssh-dsa** hostkey algorithm is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration.
Options
The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Configuring Junos OS User Accounts by Using a Configuration Group</th>
<th>102</th>
</tr>
</thead>
</table>

class
user-defined-option-82

Syntax

```
user-defined-option-82 string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides user-defined-option82 string],
[edit forwarding-options dhcp-relay group group-name overrides user-defined-option82 string],
[edit forwarding-options dhcp-relay overrides user-defined-option82 string]
```

Release Information

Statement introduced in Junos OS Release 17.2 for QFX Series switches.

Description

Configure a custom text string to use as the interface description in the DHCP option 82 Agent Circuit ID (suboption 1) information. This text string is defined independently of the interface description that is configured using the `description` statement at the `[edit interfaces interface-name]` hierarchy level.

The custom text string is configured using the `user-defined-option-82` statement at the following hierarchy levels:

- To configure a custom string on an interface level:

  ```
  [edit forwarding-options dhcp-relay group group-name interface interface-name overrides user-defined-option82 string]
  ```

- To configure a custom string at the group level:

  ```
  [edit forwarding-options dhcp-relay group group-name overrides user-defined-option82 string]
  ```

- To configure a custom string globally:

  ```
  [edit forwarding-options dhcp-relay overrides user-defined-option82 string]
  ```

You can define a custom string up to 251 characters in length. To include the custom string in the DHCP option 82 Agent Circuit ID, you must configure the `user-defined` statement at the `[edit forwarding-options dhcp-relay group group-name relay-option-82 circuit-id]` hierarchy level.

Required Privilege Level

2404
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Including a Textual Description in DHCP Options
Using DHCP Relay Agent Option 82 Information | 739
**user-id**

**Syntax**

```
user-id {ascii ascii hexadecimal hexadecimal};
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-identifier]
```

**Release Information**
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

**Description**
Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.

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

**RELATED DOCUMENTATION**
user-keepalive

Syntax

user-keepalive minutes;

Hierarchy Level

[edit services captive-portal interface (all | interface-names)]

Release Information

Statement introduced in Junos OS Release 16.1 for EX Series switches.

Description

The user-keepalive statement is used to extend a captive portal authentication session after the MAC table aging timer expires. The keep-alive timer is started when the MAC address of the authenticated host ages out of the Ethernet switching table. If traffic is received within the keep-alive timeout period, the timer is deleted. If there is no traffic within the keep-alive timeout period, the session is deleted, and the host must re-authenticate.

Default

Disabled. The captive portal authentication session ends when the associated MAC address ages out of the Ethernet switching table.

Options

minutes—Duration of keep-alive period.

Range: 7 through 65535

Required Privilege Level

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

RELATED DOCUMENTATION

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
Configuring Captive Portal Authentication (CLI Procedure) | 492
Understanding Authentication Session Timeout | 370
user-prefix (DHCP Local Server)

Syntax

user-prefix user-prefix-string;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options
user-prefix-string—User prefix string.

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

RELATED DOCUMENTATION
- Using External AAA Authentication Services with DHCP | 833
username-include (DHCP Local Server)

Syntax

```plaintext
username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description (device-interface | logical-interface);
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6 authentication],
[edit system services dhcp-local-server dhcpv6 group group-name authentication],
[edit system services dhcp-local-server group group-name authentication]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
`vlan-tags` option added in Junos OS Release 18.3R1 on MX Series routers.

Description

Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the
router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The following statements are not supported in the DHCPv6 hierarchy levels:

- option-60
- option-82

The following statements are supported in the DHCPv6 hierarchy levels only:

- client-id
- relay-agent-interface-id
- relay-agent-remote-id
- relay-agent-subscriber-id

Options

**vlan-tags**—Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format `outer-vlan-tag-inner-vlan-tag`. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

| Using External AAA Authentication Services with DHCP | 833 |
| Creating Unique Usernames for DHCP Clients | 834 |
username-include (DHCP Relay Agent)

Syntax

username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description (device-interface | logical-interface);
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
}

Hierarchy Level

[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication],
[edit forwarding-options dhcp-relay group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Support at the [edit ... dual-stack-group dual-stack-group-name] hierarchy level introduced in Junos OS Release 15.1.

vlan-tags option added in Junos OS Release 18.3R1 on MX Series routers.
Description
Configure the username that the router (or switch) passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS. Use the statement at the [edit...dhcppv6] hierarchy levels to configure DHCPv6 support.

The following statements are not supported in the DHCPv6 hierarchy levels:

- option-60
- option-82

The following statements are supported in the DHCPv6 hierarchy levels only:

- client-id
- relay-agent-interface-id
- relay-agent-remote-id
- relay-agent-subscriber-id

Options

**vlan-tags**—Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format `outer-vlan-tag-inner-vlan-tag`. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the **interface-name** option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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

**RELATED DOCUMENTATION**

- Creating Unique Usernames for DHCP Clients | 834
- Using External AAA Authentication Services with DHCP | 833
vendor-id

Syntax

vendor-id vendor-id;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family dhcp-client]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.
Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-clinet at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

Description
Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

Options
vendor-id—Vendor class ID.

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

RELATED DOCUMENTATION
**vendor-option**

**Syntax**

```plaintext
vendor-option {
  default-local-server-group local-server-group-name |
  default-relay-server-group server-group-name
  drop;
  equals
  starts-with
}
```

**Hierarchy Level**

```plaintext
[edit forwarding-options dhcp-relay relay-option-60]
```

**Release Information**

Statement introduced before Junos OS Release 12.1 for EX Series switches.
Statement deprecated in Junos OS Release 12.3 for EX Series switches.

**Description**

Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

**NOTE:** The **vendor-option** statement has been deprecated and might be removed from future product releases. We recommend that you phase out its use. See **option-number**.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) | 783
- Understanding the Extended DHCP Relay Agent for EX Series Switches
vendor-option

Syntax

vendor-option {
  (default-relay-server-group server-group-name | default-local-server-group local-server-group-name | drop);
  (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
    (drop | local-server-group local-server-group-name | relay-server-group server-group-name);
  }
}

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option-60],
[edit forwarding-options dhcp-relay group group-name relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-60],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-60],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-60]

Release Information
Statement introduced in JUNOS Release 9.0.

Description
Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

The vendor-option statement enables you to specify either an exact, left-to-right match (with the equals statement) or a partial match (with the starts-with statement), and configure either an ASCII match string (with the ascii statement) or a hexadecimal match string (with the hexadecimal statement).

You can configure an unlimited number of match strings. Match strings do not support the use of wildcard attributes.

Options

equals—Exact, left-to-right match of the ASCII or hexadecimal match string with the option 60 string.
starts-with—Partial match of the ASCII or hexadecimal match string with the option 60 string. The option 60 string can contain a superset of the ASCII or hexadecimal match string, provided that the leftmost characters of the option 60 string entirely match the characters in the configured match string. When you use the starts-with statement, the longest match rule applies; that is, the router matches the string “test123” before it matches the string “test”.

ascii match-string—ASCII match string of 1 through 255 alphanumeric characters.

hexadecimal match-hex—Hexadecimal match string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
version (BFD)

Syntax

```
version (0 | 1 | automatic);
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp oam bfd-liveness-detection],
[edit logical-systems logical-system-name protocols ldp oam fec address bfd-liveness-detection],
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd],
[edit protocols ldp oam bfd-liveness-detection],
[edit protocols ldp oam fec address bfd-liveness-detection]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the BFD protocol version to detect.

Options

- **0**—Use BFD protocol version 0.
- **1**—Use BFD protocol version 1.
- **automatic**—Autodetect the BFD protocol version.

Default: automatic

Required Privilege Level

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

RELATED DOCUMENTATION
| Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 869 |
| Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 862 |

*Configuring BFD for LDP LSPs*
version (SNMP)

Syntax

version (all | v1 | v2);

Hierarchy Level

[edit snmp trap-group group-name]

Release Information
Statement introduced before Junos OS Release 7.4 for MX, M, T, ACX and PTX Series routers, EX Series switches and SRX firewalls.
Statement introduced in Junos OS Release 9.0 for EX4600 switches.
Statement introduced in Junos OS Release 14.1X53-D20 for OCX1100 switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify the version number of SNMP traps.

Default
all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options
all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

v1—Send SNMPv1 traps only.

v2—Send SNMPv2 traps only.

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

RELATED DOCUMENTATION

Configuring SNMP Trap Groups

Configuring SNMP Trap Groups
versioning

Syntax

versioning;

Hierarchy Level

[edit system dynamic-profile-options]

Release Information
Statement introduced in Junos OS Release 11.4.

Description
Enable version support for dynamic profiles on the system.

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

RELATED DOCUMENTATION

Versioning for Dynamic Profiles

view-configuration

Can view all of the configuration (not including secrets).

Commands

No associated CLI commands.

Configuration Hierarchy Levels
No associated CLI configuration hierarchy levels and statements.

RELATED DOCUMENTATION

Understanding Junos OS Access Privilege Levels | 118
Example: Configuring User Permissions with Access Privilege Levels | 124
Example: Configuring User Permissions with Access Privileges for Operational Mode Commands | 145
Example: Configuring User Permissions with Access Privileges for Configuration Statements and Hierarchies | 160
**vlan (VoIP)**

**Syntax**

```plaintext
text
```

**Hierarchy Level**

```plaintext
[edit ethernet-switching-options voip interface (VoIP) (all | [interface-name | access-ports])
```

**Release Information**

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

**Description**

(EX Series switches only) Specify the VLAN name or VLAN tag identifier associated with the VLAN to be sent from the authenticating server to the IP phone.

**Options**

- `vlan-name`—Name of a VLAN.
- `vlan-id`—The VLAN tag identifier.
- `untagged`—Allow untagged VLAN traffic.

**Range:** 0 through 4095. Tags 0 and 4095 are reserved by Junos OS; do not configure them.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication | 550
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support | 544
**vlan-assignment**

**Syntax**

```bash
vlan-assignment (vlan-id | vlan-name);
```

**Hierarchy Level**

```bash
[edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X) mac-address];
[edit ethernet-switching-options authentication-whitelist];
[edit switch-options authentication-whitelist]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

**Description**

Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.

**Options**

`vlan-id | vlan-name`—The name of the VLAN or the VLAN tag identifier to associate with the device. The VLAN already exists on the switch.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- show dot1x static-mac-address | 2658
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Understanding Authentication on Switches | 361
**vlan-name-tlv-option**

**Syntax**

```
vlan-name-tlv-option (name | vlan-id);
```

**Hierarchy Level**

```
[edit protocols lldp]
```

**Release Information**

Statement introduced in Junos OS Release 15.1X53-D59 and 18.2R1 for EX3400 and EX4300 switches.

**Description**

Select whether to transmit the VLAN name or simply the VLAN ID for the LLDP VLAN name TLV when exchanging LLDP messages.

The switch transmits the VLAN ID by default if this statement is not configured or when you configure this statement with the `vlan-id` option. To transmit the VLAN name instead, configure this statement with the `name` option.

**Default**

VLAN ID is transmitted for the LLDP VLAN name TLV

**Options**

- **name**—The switch transmits the VLAN name for the LLDP VLAN name TLV, and the `show lldp detail` command output displays the VLAN name in the `Vlan-name` column.

- **vlan-id**—The switch transmits the VLAN ID for the LLDP VLAN name TLV, and the `show lldp detail` command output displays the default VLAN name string `vlan-vlan-id` in the `Vlan-name` column.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- `show lldp` | 2680
- Configuring LLDP (CLI Procedure) | 654
voip

Syntax

```
voip {
    interface (all | [interface-name | access-ports]) {
        vlan vlan-name;
        forwarding-class <assured-forwarding | best-effort | expedited-forwarding | network-control>;
    }
}
```

Hierarchy Level

```
[edit ethernet-switching-options];
[edit switch-options]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description

Configure VoIP interfaces.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication | 550
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support | 544
vpn (Forwarding Options)

Syntax

```
vpn;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement changed from `vpn` to `source-ip-change` in Junos OS Release 15.1X49-D130 and later releases.

Description

For Dynamic Host Configuration Protocol (DHCP) client request forwarding, enable source IP change for the device to use address of egress interface as source IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

- DHCP Overview | 909
wait-for-acct-on-ack (Access Profile)

Syntax

wait-for-acct-on-ack;

Hierarchy Level

[edit access profile profile-name accounting]

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the router’s authd process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

At subscriber session startup, the Junos OS authd process sends an Acct-On message to the RADIUS server and the new session starts authentication and accounting operations. However, in some service provider environments, upon receipt of the Acct-On message, the RADIUS server cleans up the previous session state and removes accounting statistics. In this scenario, the RADIUS server’s cleanup operation can inadvertently delete the new session’s authentication and accounting information, which might include customer billing information.

To ensure that the new session’s authentication and accounting information is not deleted, you can include the `wait-for-acct-on-ack` statement to configure authd to wait for an Acct-On-Ack response message from the RADIUS accounting server, so the RADIUS cleanup can finish before authd sends any new authentication and accounting updates.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Per-Subscriber Session Accounting
- RADIUS Servers and Parameters for Subscriber Access
watchdog

Syntax

```yaml
watchdog {
  disable;
  enable;
  timeout value;
}
```

Hierarchy Level

```plaintext
[edit system processes]
```

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Enable or disable the watchdog timer when Junos OS encounters a problem.

Options
- **disable**—Disable the watchdog timer.
- **enable**—Enable the watchdog timer.
- **timeout value**—Specify amount of time to wait in seconds.
  Range: 1 through 3600 seconds.

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

Syntax

```plaintext
web-management {
    http {
        interfaces [ interface-names ];
        port port;
    }
    https {
        interfaces [ interface-names ];
        local-certificate name;
        port port;
    }
}
```

Hierarchy Level

```
[edit system services]
```

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

Description
Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level
system—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Secure Management Access Configuration Summary
- J-Web Interface User Guide
web-management (System Processes)

Syntax

```
web-management {
    disable;
    failover (alternate-media | other-routing-engine);
}
```

Hierarchy Level

```
[edit system processes]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Specify the Web management process.

Options

- `disable`—Disable the Web management process.
- `failover`—Configure the device to reboot if the software process fails four times within 30 seconds, and specify the software to use during the reboot.
  - `alternate-media`—Configure the device to switch to backup media that contains a version of the system if a software process fails repeatedly.
  - `other-routing-engine`—Instruct the secondary Routing Engine to take mastership if a software process fails. If this statement is configured for a process, and that process fails four times within 30 seconds, then the device reboots from the secondary Routing Engine.

Required Privilege Level

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.
web-management (System Services)

Syntax

```plaintext
web-management {
  http {
    interfaces interface-names;
    port port;
  }
  https {
    interfaces interface-names;
    local-certificate name;
    pki-local-certificate name;
    system-generated-certificate name;
    port port;
  }
  management url management-url;
  session {
    idle-timeout minutes;
    session-limit number;
  }
  traceoptions {
    file {
      filename;
      files number;
      match regular-expression;
      size maximum-file-size;
      (no-world-readable | world-readable);
    }
    flag flag;
    level level;
    no-remote-trace;
  }
}
```

Hierarchy Level

[edit system services]

Release Information

Statement introduced in Junos OS Release 9.0.
Support for **https** introduced for SRX5400, SRX5600, and SRX5800 devices starting from Junos OS Release 12.1X44-D10 and on vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices starting from Junos OS Release 15.1X49-D40.

**Description**

Configure settings for HTTP or HTTPS access. HTTP access allows management of the device using the J-Web interface. HTTPS access allows secure management of the device using the J-Web interface. With HTTPS access, communication is encrypted between your browser and the webserver for your device.

**NOTE:** On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use ge and fxp0 ports as management ports, you must use the set system services web-management http command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from ge-0/0/1.0 through ge-0/0/7.0.
Options

control—Disable the SBC process.

- **max-threads**—Maximum simultaneous threads to handle requests.

  Range: 0 through 16

http—Configure HTTP.

- **interface [value]**—Interface value that accepts HTTP access.
- **port number**—TCP port for incoming HTTP connections.

  Range: 1 through 65,535

https—Configure HTTPS.

- **interface [value]**—Interface value that accept HTTP access.
- **port number**—TCP port for incoming HTTP connections.

  Range: 1 through 65,535
- **local-certificate**—X.509 certificate to use from the configuration.
- **pki-local-certificate**—X.509 certificate to use from the PKI local store.
- **system-generated-certificate**—X.509 certificate generated automatically by the system.

management url management url—URL path for Web management access.

session—Configure the Web-management session.

- **idle-timeout minutes**—Default timeout of Web-management sessions in minutes.
- **session-limit number**—Maximum number of Web-management sessions to allow.

traceoptions—Set the trace options.

- **file**—Configure the trace file information.
  - **filename**—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory /var/log. By default, the name of the file is the name of the process being traced.
  - **files number**—Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

    If you specify a maximum number of files, you also must specify a maximum file size with the **size maximum file-size** option.
Range: 2 through 1000 files

Default: 10 files

- match regular-expression — Refine the output to include lines that contain the regular expression.
- size maximum-file-size — Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Range: 10 KB through 1 GB

Default: 128 KB

If you specify a maximum file size, you also must specify a maximum number of trace files with the files number option.

- (world-readable | no-world-readable) — By default, log files can be accessed only by the user who configures the tracing operation. The world-readable option enables any user to read the file. To explicitly set the default behavior, use the no-world-readable option.

- flag flag — Specify which tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags.

- all—Trace all areas.
- configuration—Trace configuration.
- dynamic-vpn—Trace dynamic VPN events.
- init—Trace the daemon init process.
- mgd—Trace MGD requests.
- webauth—Trace Web authentication requests.

- level level — Specify the level of debugging output.

- all—Match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match conditions that should be handled specially.
- verbose—Match verbose messages.
- warning—Match warning messages.
- no-remote-trace—Disable remote tracing.

Required Privilege Level

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

Firewall User Authentication Overview

Dynamic VPN Overview
what

**Syntax**

```
what number;
```

**Hierarchy Level**

```
[edit protocols lldp-med interface (all | interface-name) location civic-based]
```

**Release Information**


**Description**

For Link Layer Discovery Protocol–Media Endpoint Device (LLDP-MED), configure the location to which the DHCP entry refers. This information is advertised, along with other location information, from the switch to the MED. It is used during emergency calls to identify the location of the MED.

Options 0 and 1 should not be used unless it is known that the DHCP client is in close physical proximity to the server or network element.

**Default**

1

**Options**

`number`—Location:

- 0—Location of the DHCP server.
- 1—Location of a network element believed to be closest to the client.
- 2—Location of the client.

**Required Privilege Level**

routing—To view this statement in the configuration.

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

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>show lldp</th>
<th>2680</th>
</tr>
</thead>
</table>

Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch | 528
wins-server (System)

Syntax

wins-server {
    address;
}

Hierarchy Level

[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

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

Description
For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as 192.168.1.3) to Windows NetBIOS names (such as \Marketing). List servers in order of preference.

Options
address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple address options.

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

RELATED DOCUMENTATION
**xnm-clear-text**

**Syntax**

```plaintext
xnm-clear-text {
  connection-limit limit;
  rate-limit limit;
}
```

**Hierarchy Level**

[edit system services]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Allow Junos XML protocol clear-text requests from remote systems to the local router.

**NOTE:** Junos OS Evolved does not support the `xnm-clear-text` statement.

The remaining statements are explained separately.

**Required Privilege Level**

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

**RELATED DOCUMENTATION**

- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*
**xnm-ssl**

**Syntax**

```
    xnm-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
        ssl-renegotiation;
    }
```

**Hierarchy Level**

```
    [edit system services]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Support for the `ssl-renegotiation` statement added in Junos OS Release 13.3.

**Description**

Allow Junos XML protocol SSL requests from remote systems to the local router.

The remaining statements are explained separately.

**WARNING:** Starting with Junos OS Release 15.1, the `sslv3-support` option is not available for configuration with the `set system services xnm-ssl` and `file copy` commands. SSLv3 is no longer supported and available.

For all releases prior to and including Junos OS Release 14.2, SSLv3 is disabled by default at runtime. The `sslv3-support` option is hidden and deprecated in Junos OS Release 14.2 and earlier releases. However, you can use the `set system services xnm-ssl sslv3-support` command to enable SSLv3 for a Junos XML protocol client application to use as the protocol to connect to the Junos XML protocol server on a router, and you can use the `file copy source destination sslv3-support` command to enable the copying of files from an SSLv3 URL.

Using SSLv3 presents a potential security vulnerability, and we recommend that you not use SSLv3. For more details about this security vulnerability, go to https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10656.
NOTE: When FIPS mode is enabled on the device, the xnm-ssl service does not support TLS 1.0. For a device in FIPS mode, the clients must communicate with the xnm-ssl service using TLS 1.1 or later. In non-FIPS mode, clients can communicate with the xnm-ssl service using TLS 1.0 or later. The xnm-ssl service never negotiates with the SSLv2 or SSLv3 (the predecessors to TLS 1.0) even if the FIPS mode is enabled or disabled.

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

RELATED DOCUMENTATION
Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
16

CHAPTER

Operational Commands

clear accounting server statistics archival-transfer | 2451

clear captive-portal | 2452

clear dhcp client binding | 2455

clear dhcp client statistics | 2456

clear dhcp relay binding | 2457

clear dhcp relay statistics | 2458

clear dhcp server binding | 2459

clear dhcp server statistics | 2460

clear dhcpv6 client binding | 2461

clear dhcpv6 client statistics | 2462

clear dhcpv6 relay binding | 2463

clear dhcpv6 relay statistics | 2467

clear dhcpv6 server binding | 2470

clear dhcpv6 server binding (Local Server) | 2473

clear dhcpv6 server statistics | 2474
clear dhcpv6 server statistics (Local Server) | 2476

clear dot1x | 2477

clear lldp neighbors | 2480

clear lldp statistics | 2481

clear lldp neighbors | 2482

clear lldp statistics | 2483

clear network-access radsec state | 2484

clear network-access radsec statistics | 2485

clear security pki local-certificate | 2486

clear security ssh key-pair-identity | 2488

clear system login lockout | 2489

clear system services dhcp binding | 2490

clear system services dhcp conflict | 2491

clear system services dhcp statistics | 2492

request component login | 2493

request dhcp client renew | 2496

request dhcp server reconfigure | 2497

request dhcpv6 server reconfigure | 2499

request dhcpv6 client renew | 2501

request ipsec switch | 2502

request message | 2503

request security certificate enroll (Signed) | 2505

request security certificate enroll (Unsigned) | 2507

request security key-pair | 2509

request security pki generate-key-pair | 2511

request security pki local-certificate generate-self-signed | 2513

request security ssh key-pair-identity generate | 2515

request security tpm master-encryption-password set | 2517

request system autorecovery state | 2519
request system decrypt password | 2522
request system download abort | 2524
request system download clear | 2526
request system download pause | 2527
request system download resume | 2529
request system download start | 2531
request system firmware upgrade | 2533
request system license update | 2535
request system reboot | 2537
request system reboot (SRX Series) | 2547
request system services dhcp | 2549
request system snapshot (Maintenance) | 2550
request system software abort in-service-upgrade (ICU) | 2554
request system software add (Maintenance) | 2556
request system software rollback (SRX Series) | 2557
request system zeroize | 2558
restart (Reset) | 2560
show accounting server statistics archival-transfer | 2565
show captive-portal authentication-failed-users | 2566
show captive-portal firewall | 2568
show captive-portal interface | 2571
show chassis routing-engine (View) | 2576
show dhcp client binding | 2582
show dhcp client statistics | 2586
show dhcp relay binding | 2590
show dhcp relay statistics | 2593
show dhcp server binding | 2595
show dhcp server statistics | 2597
show dhcpv6 client binding | 2600
show dhcpv6 client statistics | 2603
show dhcpv6 relay binding | 2606
show dhcpv6 relay statistics | 2617
show dhcpv6 server binding | 2622
show dhcpv6 server binding (View) | 2630
show dhcpv6 server statistics | 2636
show dhcpv6 server statistics (View) | 2640
show dot1x | 2644
show dot1x accounting attribute | 2651
show dot1x authentication-failed-users | 2654
show dot1x firewall | 2656
show dot1x static-mac-address | 2658
show dot1x statistics | 2660
show ethernet-switching interface | 2663
show ethernet-switching interfaces | 2667
show firewall (View) | 2677
show lldp | 2680
show lldp local-information | 2688
show lldp neighbors | 2691
show lldp neighbors | 2697
show lldp remote-global-statistics | 2705
show lldp statistics | 2707
show lldp statistics | 2709
show network-access aaa statistics accounting | 2712
show network-access aaa statistics authentication | 2714
show network-access aaa statistics dynamic-requests | 2716
show network-access radsec local-certificate | 2718
show network-access radsec statistics | 2721
show network-access radsec state | 2724
show route extensive  | 2727
show route instance  | 2753
show route protocol  | 2758
show security ssh key-pair-identity  | 2776
show security pki local-certificate  | 2778
show security tpm status  | 2782
show services unified-access-control authentication-table  | 2784
show services unified-access-control policies  | 2787
show services unified-access-control status  | 2790
show snmp  | 2791
show snmp statistics  | 2794
show ssl-certificates  | 2802
show subscribers  | 2805
show system autorecovery state  | 2854
show system download  | 2856
show system license (View)  | 2858
show system login lockout  | 2862
show system services dhcp binding  | 2864
show system services dhcp client  | 2867
show system services dhcp conflict  | 2871
show system services dhcp global  | 2873
show system services dhcp pool  | 2875
show system services dhcp relay-statistics  | 2878
show system services dhcp statistics  | 2880
show system services service-deployment  | 2883
show system snapshot media  | 2885
show system storage partitions  | 2888
show system users  | 2892
ssh  | 2898
telnet | 2901

test access profile | 2904

test access radius-server | 2909
clear accounting server statistics archival-transfer

**Syntax**

```
clear accounting server statistics archival-transfer
```

**Release Information**
Command introduced in Junos OS Release 19.2.

**Description**
Clears the statistics of transfer attempted, succeeded, and failed for accounting statistics files and router configuration archives.

**Options**
This command has no options.

**Required Privilege Level**
clear

**Output Fields**
When you enter this command, the transfer statistics are cleared.

**Sample Output**
```
clear accounting server statistics archival-transfer
user@host> clear accounting server statistics archival-transfer
```
clear captive-portal

Syntax

```
clear captive-portal (firewall [interface-names] | interface (802.1X) (all | [interface-names])) | mac-address [mac-addresses])
```

Release Information
Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description
Reset the authentication state of a captive portal interface or captive portal firewall statistics on one or more interfaces.

Options

- **firewall [interface-names]**—Resets captive portal statistics on all interfaces or on the specified interface.
- **interface (all | [interface-names])**—Resets the authentication state of users connected to all interfaces or the specified interfaces.
- **mac-address mac-addresses**—Resets the authentication state for the specified MAC addresses.

Required Privilege Level
view

RELATED DOCUMENTATION

- show captive-portal authentication-failed-users | 2566
- show captive-portal interface | 2571
- show captive-portal firewall | 2568
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492

List of Sample Output
- clear captive-portal interface on page 2453
- clear captive-portal interface on page 2453
- clear captive-portal mac-address on page 2454
- clear captive-portal firewall on page 2454
Output Fields

Table 62 on page 2453 lists the output fields for the clear captive-portal interface command. (The clear captive-portal firewall and clear captive-portal mac-address commands have no output). Output fields are listed in the approximate order in which they appear.

Table 62: clear captive-portal interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which captive portal has been configured.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the port:</td>
</tr>
<tr>
<td></td>
<td>• Authenticated—The client has been authenticated through the RADIUS server or has</td>
</tr>
<tr>
<td></td>
<td>been permitted access through server fail fallback.</td>
</tr>
<tr>
<td></td>
<td>• Authenticating—The client is authenticating through the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>• Connecting—Switch is attempting to contact the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>• Initialize—The interface link is down.</td>
</tr>
<tr>
<td></td>
<td>• Held—An action has been triggered through server fail fallback during a RADIUS</td>
</tr>
<tr>
<td></td>
<td>server timeout. A supplicant is denied access, permitted access through a specified</td>
</tr>
<tr>
<td></td>
<td>VLAN, or maintains the authenticated state granted to it before the RADIUS server</td>
</tr>
<tr>
<td></td>
<td>timeout occurred.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the connected client on the interface.</td>
</tr>
<tr>
<td>User</td>
<td>Users connected to the captive portal interface.</td>
</tr>
</tbody>
</table>

Sample Output

clear captive-portal interface

user@switch> clear captive-portal interface

ge-0/0/3.0

clear captive-portal interface

user@switch> clear captive-portal interface

<table>
<thead>
<tr>
<th>Captive Portal Information:</th>
<th>MAC address</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>State</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>Authenticated</td>
<td>00:03:47:el:ba:b9</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>Connecting</td>
<td></td>
</tr>
</tbody>
</table>
clear captive-portal mac-address

user@switch> clear captive-portal mac-address 00:03:47:e1:ba:b9

This command has no output.

clear captive-portal firewall

user@switch> clear captive-portal firewall

This command has no output.
clear dhcp client binding

Syntax

```
clear dhcp client binding
   [all|interface <interface-name>]
   [routing-instance <routing-instance-name>]
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.

Options
all—(Optional) Clear the binding state for all DHCP clients.

interface <interface-name>—(Optional) Clear the binding state for DHCP clients on the specified interface.

routing-instance <routing-instance-name>—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

```
show dhcp client binding | 2582
```

Output Fields
This command produces no output.
clear dhcp client statistics

Syntax

```
clear dhcp client statistics
<all>
@interface>
<routing-instance>
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.

Options

**all**—(Optional) Clear all the DHCP client statistics.

**interface**—(Optional) Clear the statistics for DHCP clients on the specified interface.

**routing-instance**—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

| show dhcp client statistics | 2586 |

Output Fields
This command produces no output.
clear dhcp relay binding

Syntax

```bash
clear dhcp relay binding
<all | ip-address | mac-address>
@interface interface-name>
<routing-instance routing-instance-name>
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.

Options
all—(Optional) Clear the binding state for all DHCP clients.

ip-address—(Optional) Clear the binding state for the DHCP client, using the specified IP address.

mac-address—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.

interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.

routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

- show dhcp relay binding | 2590

Output Fields
This command produces no output.
clear dhcp relay statistics

Syntax

```
clear dhcp relay statistics
  <routing-instance routing-instance-name>
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options
**routing-instance routing-instance-name**—(Optional) Clear the DHCP relay statistics on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

```
| show dhcp relay statistics | 2593 |
```

Output Fields
This command produces no output.
clear dhcp server binding

Syntax

```
clear dhcp server binding
<all | ip-address | mac-address>
<intface interface-name>
<routing-instance routing-instance-name>
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.

Options
- **all**—(Optional) Clear the binding state for all DHCP clients.
- **ip-address**—(Optional) Clear the binding state for the DHCP client, using the specified IP address.
- **mac-address**—(Optional) Clear the binding state for the DHCP client, using the specified MAC address.
- **interface interface-name**—(Optional) Clear the binding state for DHCP clients on the specified interface.
- **routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level
- clear

RELATED DOCUMENTATION
- show dhcp server binding | 2595

Output Fields
This command produces no output.
clear dhcp server statistics

Syntax

clear dhcp server statistics
<routing-instance routing-instance-name>

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

routing-instance routing-instance-name—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

| show dhcp server statistics | 2597 |

Output Fields
This command produces no output.
clear dhcpv6 client binding

Syntax

```
clear dhcpv6 client binding
    [all | interface interface-name]
    [routing-instance routing-instance-name]
```

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table.

Options
- `all`—(Optional) Clear the binding state for all DHCPv6 clients.
- `interface interface-name`—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- `routing-instance routing-instance-name`—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for DHCPv6 clients on the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

```
show dhcpv6 client binding | 2600
```

Output Fields
This command produces no output.
clear dhcpv6 client statistics

Syntax

```
clear dhcpv6 client statistics
    routing-instance routing-instance-name
```
clear dhcpv6 relay binding

Syntax

```xml
clear dhcpv6 relay binding
  <address>
  <all>
  <dual-stack>
  <interface interface-name>
  <interfaces-vlan>
  <interfaces-wildcard>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Option `dual-stack` added in Junos OS Release 15.1.

Description

Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.

Options

`address`—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:

- CID—The specified Client ID (CID).
- ipv6-prefix—The specified IPv6 prefix.
- session-id—The specified session ID.

`all`—(Optional) Clear the binding state for all DHCPv6 clients.

`dual-stack`—(Optional) Clear the binding state for DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.

`interfaces-vlan`—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

`interfaces-wildcard`—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character ("*").

`interface interface-name`—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
**logical-system logical-system-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.

**routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**

Viewing and Clearing DHCP Bindings

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dhcpv6 relay binding</td>
<td>2606</td>
</tr>
</tbody>
</table>

**List of Sample Output**

- clear dhcpv6 relay binding on page 2464
- clear dhcpv6 relay binding <prefix> on page 2465
- clear dhcpv6 relay binding all on page 2465
- clear dhcpv6 relay binding dual-stack all on page 2465
- clear dhcv6p relay binding interface on page 2466
- clear dhcpv6 relay binding <interfaces-vlan> on page 2466
- clear dhcpv6 relay binding <interfaces-wildcard> on page 2466

**Output Fields**

See show dhcpv6 relay binding for an explanation of output fields.

**Sample Output**

**clear dhcpv6 relay binding**

The following sample output displays the DHCPv6 bindings before and after the clear dhcpv6 relay binding command is issued.

```
user@host> show dhcpv6 relay binding

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:3c4d:15::/64</td>
<td>1</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:3c4d:16::/64</td>
<td>2</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
</tbody>
</table>
```

"2464"
clear dhcpv6 relay binding <prefix>

user@host> clear dhcpv6 relay binding 2001:db8:3c4d:15::/64

user@host> show dhcpv6 relay binding

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:3c4d:16::/64</td>
<td>2</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:3c4d:17::/64</td>
<td>3</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03</td>
</tr>
<tr>
<td>2001:db8:3c4d:18::/64</td>
<td>4</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04</td>
</tr>
<tr>
<td>2001:db8:3c4d:19::/64</td>
<td>5</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05</td>
</tr>
<tr>
<td>2001:db8:3c4d:20::/64</td>
<td>6</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06</td>
</tr>
</tbody>
</table>

clear dhcpv6 relay binding all

The following command clears all DHCP relay agent bindings:

user@host> clear dhcpv6 relay binding all

clear dhcpv6 relay binding dual-stack all

The following command clears all DHCPv6 relay agent bindings for all DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.

user@host> clear dhcpv6 relay binding dual-stack all
clear dhcv6p relay binding interface
The following command clears DHCPv6 relay agent bindings on a specific interface:

user@host> clear dhcv6 relay binding interface fe-0/0/2

clear dhcv6 relay binding <interfaces-vlan>
The following command uses the interfaces-vlan option to clear all DHCPv6 relay agent bindings on top of the underlying interface ae0, which clears DHCPv6 bindings on all demux VLANs on top of ae0:

user@host> clear dhcv6 relay binding interface ae0

clear dhcv6 relay binding <interfaces-wildcard>
The following command uses the interfaces-wildcard option to clear all DHCPv6 relay agent bindings over a specific interface:

user@host> clear dhcv6 relay binding ge-1/0/0.*
clear dhcpv6 relay statistics

Syntax

```
clear dhcpv6 relay statistics
<bulk-leasequery-connections>
<leasequery>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information
Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description
Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options
bulk-leasequery-connections—(Optional) Clear DHCPv6 relay bulk leasequery statistics.
leasequery—(Optional) Clear DHCPv6 relay individual leasequery statistics.
logical-system logical-system-name—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system.
routing-instance routing-instance-name—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege Level
view

List of Sample Output
clear dhcpv6 relay statistics on page 2468

Output Fields
See show dhcpv6 relay statistics for an explanation of output fields.
Sample Output

clear dhcpv6 relay statistics

The following sample output displays the DHCPv6 relay statistics before and after the `clear dhcpv6 relay statistics` command is issued.

```
user@host> show dhcpv6 relay statistics

DHCPv6 Packets dropped:
   Total                       0
   Lease Time Violated         1

Messages received:
   DHCPV6_DECLINE              0
   DHCPV6_SOLICIT              10
   DHCPV6_INFORMATION_REQUEST  0
   DHCPV6_RELEASE              0
   DHCPV6_REQUEST              10
   DHCPV6_CONFIRM              0
   DHCPV6_RENEW                0
   DHCPV6_REBIND               0
   DHCPV6_RELAY_REPL           0

Messages sent:
   DHCPV6_ADVERTISE            0
   DHCPV6_REPLY                0
   DHCPV6_RECONFIGURE          0
   DHCPV6_RELAY_FORW           0

user@host> clear dhcpv6 relay statistics

user@host> show dhcpv6 relay statistics

DHCPv6 Packets dropped:
   Total                       0

Messages received:
   DHCPV6_DECLINE              0
   DHCPV6_SOLICIT              0
   DHCPV6_INFORMATION_REQUEST  0
   DHCPV6_RELEASE              0
   DHCPV6_REQUEST              0
   DHCPV6_CONFIRM              0
   DHCPV6_RENEW                0
```
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPV6_REBIND</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RELAY_REPL</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_ADVERTISE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_REPLY</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RECONFIGURE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RELAY_FORW</td>
<td>0</td>
</tr>
</tbody>
</table>

Messages sent:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPV6_REBIND</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RELAY_REPL</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_ADVERTISE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_REPLY</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RECONFIGURE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPV6_RELAY_FORW</td>
<td>0</td>
</tr>
</tbody>
</table>
clear dhcpv6 server binding

Syntax

clear dhcpv6 server binding
  <address>
  <all>
  <interface interface-name>
  <interfaces-vlan>
  <interfaces-wildcard>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
  <dual-stack>

Release Information
Options interfaces-vlan and interfaces-wildcard added in Junos OS Release 12.1.
Command updated with dual-stack statement in Junos OS Release 17.3.

Description
Clear the binding state of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client from the client table on the extended DHCPv6 local server.

Options
address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:

- CID—The specified Client ID (CID).
- ipv6-prefix—The specified IPv6 prefix.
- session-id—The specified session ID.

all—(Optional) Clear the binding state for all DHCPv6 clients.

interface interface-name—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).

logical-system logical-system-name—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.

routing-instance routing-instance-name—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.
dual-stack—(Optional) Remove either both arms or single arm of dual-stack.

**NOTE:**
- The **dual-stack** command is added in the syntax removes both arms of the dual-stack with a single command entry.
- When the **dual-stack** command is not added in the syntax, the `clear dhcpv6 server binding` command clears only the family specific arm of the dual-stack.

**Required Privilege Level**
clear

**RELATED DOCUMENTATION**

- Viewing and Clearing DHCP Bindings
  - show dhcpv6 server binding | 2622

**List of Sample Output**
- `clear dhcpv6 server binding all on page 2471`
- `clear dhcpv6 server binding <ipv6-prefix> on page 2472`
- `clear dhcpv6 server binding interface on page 2472`
- `clear dhcpv6 server binding <interfaces-vlan> on page 2472`
- `clear dhcpv6 server binding <interfaces-wildcard> on page 2472`
- `clear dhcpv6 server binding dual-stack all on page 2472`

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```plaintext
user@host> clear dhcpv6 server binding all
```

The following command clears all DHCPv6 local server bindings:
clear dhcpv6 server binding <ipv6-prefix>
The following command clears DHCPv6 local server bindings for a specific IPv6 prefix:

```
user@host> clear dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
```

clear dhcpv6 server binding interface
The following command clears DHCPv6 local server bindings on a specific interface:

```
user@host> clear dhcpv6 server binding interface fe-0/0/2
```

clear dhcpv6 server binding <interfaces-vlan>
The following command uses the `interfaces-vlan` option to clear all DHCPv6 local server bindings on top of the underlying interface `ae0`, which clears DHCPv6 bindings on all demux VLANs on top of `ae0`:

```
user@host> clear dhcpv6 server binding interface ae0
```

clear dhcpv6 server binding <interfaces-wildcard>
The following command uses the `interfaces-wildcard` option to clear all DHCPv6 local server bindings over a specific interface:

```
user@host> clear dhcpv6 server binding ge-1/0/0.*
```

clear dhcpv6 server binding dual-stack all
The following command clears all the dual-stack local server bindings.

```
user@host> clear dhcpv6 server binding dual-stack all
```
clear dhcpv6 server binding (Local Server)

Syntax

```
clear dhcpv6 server binding
  <all | client-id | ip-address | session-id>
  <interface interface-name>
  <routing-instance routing-instance-name>
```

Release Information
Command introduced in Junos OS Release 10.4.

Description
Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

Options
- **all**—(Optional) Clear the binding state for all DHCPv6 clients.
- **client-id**—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).
- **ip-address**—(Optional) Clear the binding state for the DHCPv6 client with the specified address.
- **session-id**—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.
- **interface interface-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- **routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

| show dhcpv6 server binding (View) | 2630 |
clear dhcpv6 server statistics

Syntax

```
clear dhcpv6 server statistics
<bulk-leasequery-connections>
<interface interface-name>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Description
Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options
bulk-leasequery-connections—(Optional) Clear DHCPv6 local server bulk leasequery statistics.

logical-system logical-system-name—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

routing-instance routing-instance-name—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

| show dhcpv6 server statistics | 2636 |

List of Sample Output
clear dhcpv6 server statistics on page 2475

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear dhcpv6 server statistics

user@host> clear dhcpv6 server statistics
clear dhcpv6 server statistics (Local Server)

Syntax

clear dhcpv6 server statistics
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>

Release Information
Command introduced in Junos OS Release 10.4.

Description
Clear all DHCPv6 local server statistics.

Options
logical-system logical-system-name—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

routing-instance routing-instance-name—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level
clear

RELATED DOCUMENTATION

  show dhcpv6 server statistics (View) | 2640
clear dot1x

Syntax

```
clear dot1x (firewall <counter-name> | interface <interface-name> | mac-address [mac-addresses] | statistics <interface interface-name>)
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.
`firewall` option added in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Support for `eapol-block` introduced in Junos OS Releases 14.1X53-D40 and 15.1X53-D51 for EX Series switches.

Description
Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the `interface` or `mac-address` options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the `clear dot1x interface` command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the `show dot1x interface detail` command. The values for `Reauthentication due` and `Reauthentication interval` will be about the same.

CAUTION: When you clear the learned MAC addresses from an interface using the `clear dot1x interface` command, all MAC addresses are cleared, including those in static MAC bypass list.

If you have enabled Media Access Control Security (MACsec) using static secure association key (SAK) security mode on an EX Series switch, the SAKs are rotated when the `clear dot1x` command is entered. The `clear dot1x` command has no impact on MACsec when MACsec is enabled using static connectivity association keys (CAK) or any other security mode.

Options
`eapol-block`—Clear EAPOL block on the interface and allow the switch to receive EAPOL messages from a supplicant connected to that interface.
**firewall** `<counter-name>`—Clear 802.1X firewall counter statistics. If the `counter-name` option is specified, clear 802.1X firewall statistics for that counter.

**interface** `<[interface-name]>`—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

**mac-address** `[mac-addresses]`—Reset the authentication state of the specified MAC addresses.

**statistics** `<interface interface-name>`—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the `interface` option is specified, clear 802.1X firewall statistics for that interface or interfaces.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**

- `show dot1x` | 2644
- `Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch` | 440
- `Filtering 802.1X Supplicants by Using RADIUS Server Attributes` | 395

**List of Sample Output**

clear dot1x firewall on page 2478

clear dot1x interface (Specific Interfaces) on page 2478

clear dot1x mac-address (Specific MAC Address) on page 2478

clear dot1x statistics interface (Specific Interface) on page 2479

clear dot1x eapol-block on page 2479

---

**Sample Output**

clear dot1x firewall

user@switch> clear dot1x firewall c1

clear dot1x interface (Specific Interfaces)

user@switch> clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0

clear dot1x mac-address (Specific MAC Address)

user@switch> clear dot1x mac-address 00:04:ae:cd:23:5f
clear dot1x statistics interface (Specific Interface)

user@switch> clear dot1x statistics interface ge-1/0/1

clear dot1x eapol-block

user@switch> clear dot1x eapol-block
clear lldp neighbors

Syntax

clear lldp neighbors
<interface interface>

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Clear the learned remote neighbor information on all or selected interfaces.

Options
none—Clear the remote neighbor information on all interfaces.
interface interface—(Optional) Clear the remote neighbor information from one or more selected interfaces.

Required Privilege Level
view

RELATED DOCUMENTATION

- show lldp | 2680
- Configuring LLDP (CLI Procedure) | 654
- Understanding LLDP and LLDP-MED on EX Series Switches | 661

List of Sample Output
- clear lldp neighbors on page 2480
- clear lldp neighbors interface ge-0/1/1.0 on page 2480

Sample Output

- clear lldp neighbors
  user@switch> clear lldp neighbors

- clear lldp neighbors interface ge-0/1/1.0
  user@switch> clear lldp neighbors interface ge-0/1/1.0
clear lldp statistics

Syntax

```
clear lldp statistics
<interface interface>
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Clear LLDP statistics on one or more interfaces.

Options
- **none**—Clears LLDP statistics on all interfaces.
- **interface interface-names**—(Optional) Clear LLDP statistics on one or more interfaces.

Required Privilege Level
- **view**

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Configuring LLDP (CLI Procedure)</th>
<th>654</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding LLDP and LLDP-MED on EX Series Switches</td>
<td>661</td>
</tr>
</tbody>
</table>

List of Sample Output
- clear lldp statistics on page 2481
- clear lldp statistics interface ge-0/1/1.0 on page 2481

Sample Output

```
clear lldp statistics
user@switch> clear lldp statistics

clear lldp statistics interface ge-0/1/1.0
user@switch> clear lldp statistics interface ge-0/1/1.0
```
clear lldp neighbors

Syntax

```
clear lldp neighbors <interface interface>
```

Release Information

Description
Clear the learned remote neighbor information on all or selected interfaces.

Options
none—Clear the remote neighbor information on all interfaces.

interface interface—(Optional) Clear the remote neighbor information from the selected interface.

Required Privilege Level
view

RELATED DOCUMENTATION
Understanding LLDP | 653

List of Sample Output
clear lldp neighbors on page 2482
clear lldp neighbors interface on page 2482

Sample Output

clear lldp neighbors
user@switch> clear lldp neighbors

clear lldp neighbors interface
clear lldp neighbors interface ge-0/1/0
clear lldp statistics

Syntax

clear lldp statistics
<interface interface>

Release Information
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Clear LLDP statistics on one or more interfaces.

Options

none—Clears LLDP statistics on all interfaces.

interface interface-names—(Optional) Clear LLDP statistics on an interface.

Required Privilege Level
view

RELATED DOCUMENTATION
Understanding LLDP | 653

List of Sample Output
clear lldp statistics on page 2483
clear lldp statistics interface on page 2483

Sample Output

clear lldp statistics
  user@switch> clear lldp statistics

clear lldp statistics interface
  user@switch> clear lldp statistics interface ge-0/1/0
clear network-access radsec state

Syntax

```
clear network-access radsec state
<destination destination-id>
```

Release Information
Command introduced in Junos OS Release 19.1R1.

Description
Clear the connection state information for RADSEC destinations.

Options
```
destination destination-id—(Optional) Clear connection state information for the specified RADSEC destination.
```

Required Privilege Level
clear

RELATED DOCUMENTATION
```
RADIUS over TLS (RADSEC) | 259
```

Output Fields
This command produces no output.
clear network-access radsec statistics

Syntax

```
clear network-access radsec statistics
<destination destination-id>
```

Release Information
Command introduced in Junos OS Release 19.1R1.

Description
Clear the connection statistics for RADSEC destinations.

Options

destination destination-id—(Optional) Clear connection statistics for the specified RADSEC destination.

Required Privilege Level
clear

RELATED DOCUMENTATION

- RADIUS over TLS (RADSEC) | 259

Output Fields
This command produces no output.
clear security pki local-certificate

Syntax

clear security pki local-certificate
<all | certificate-id certificate-id-name | system-generated>

Release Information
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description
Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the switch.

Options
all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

NOTE: This option does not delete the automatically generated self-signed certificate or its public/private key pair.

certificate-id certificate-id-name—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.

system-generated—(Optional) Delete the automatically generated self-signed certificate.

Required Privilege Level
clear

RELATED DOCUMENTATION

Deleting Self-Signed Certificates (CLI Procedure)  |  343

List of Sample Output
clear security pki local-certificate all on page 2487

Output Fields
This command produces no output.
Sample Output

```
clear security pki local-certificate all

user@switch> clear security pki local-certificate all
```
clear security ssh key-pair-identity

Syntax

```
clear security ssh key-pair-identity <all> | <identity-name>
```

Release Information

Command introduced in Junos OS Release 15.1X49-D70.

Description

Clear private and public SSH key pair for the specified files.

Options

- **all**—Clear all the key-pair files.
- **identity-name**—Clear identity name.

Required Privilege Level

clear

Related Documentation

- request security ssh key-pair-identity generate | 2515
- show security ssh key-pair-identity | 2776

List of Sample Output

clear security ssh key-pair-identity sample on page 2488

Output Fields

Sample Output

clear security ssh key-pair-identity sample

```
user@host> clear security ssh key-pair-identity sample

SSH key sample was removed
```
clear system login lockout

Syntax

clear system login lockout
  <all>
  <user username>

Release Information
Command introduced in Junos OS Release 11.2.

Description
Unlock the user account locked as a result of invalid login attempts.

Options
all—Clear all locked user accounts.
user username—Clear the specified locked user account.

Required Privilege Level
clear

RELATED DOCUMENTATION

| lockout-period | 1920
| show system login lockout | 2862

Output Fields
This command produces no output.
clear system services dhcp binding

**Syntax**

```
clear system services dhcp binding
<address>
```

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

**Description**
(EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool.

**Options**
- `address`—(Optional) Remove a specific IP address binding and return it to the address pool.

**Required Privilege Level**
view and system

**RELATED DOCUMENTATION**

- `show system services dhcp binding` | 2864

**List of Sample Output**
clear system services dhcp binding on page 2490

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

clear system services dhcp binding

`user@host>` clear system services dhcp binding
clear system services dhcp conflict

Syntax

```
clear system services dhcp conflict
<address>
```

Release Information

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

Description

(J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool.

Options

`address`—(Optional) Remove a specific IP address from the conflict list and return it to the address pool.

Required Privilege Level

view and system

RELATED DOCUMENTATION

```
show system services dhcp conflict  |  2871
```

List of Sample Output

clear system services dhcp conflict on page 2491

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear system services dhcp conflict
user@host> clear system services dhcp conflict
```
clear system services dhcp statistics

Syntax

```
clear system services dhcp statistics
```

Release Information

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

Description

(J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics.

Options

This command has no options.

Required Privilege Level

view and system

RELATED DOCUMENTATION

- show system services dhcp statistics | 2880

List of Sample Output

clear system services dhcp statistics on page 2492

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear system services dhcp statistics
user@host> clear system services dhcp statistics
```
request component login

Syntax

request component login component-name

Release Information

Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

(QFabric systems only) Log in to a QFabric system component. To gain access to individual components by way of the request component login command, you must first provide the qfabric-admin or qfabric-operator class privilege to your user (for more information, see: remote-debug-permission).

Options

component-name—Specify the QFabric system component to which you wish to log in.

Required Privilege Level

admin

RELATED DOCUMENTATION

List of Sample Output

request component login (with qfabric-admin Privileges) on page 2493
request component login (with qfabric-operator Privileges) on page 2494
request component login (with qfabric-user Privileges) on page 2495

Sample Output

The three sample output displays show the results of attempts to log in to Node device EE3093. The results differ depending on the privilege level assigned to the user.

request component login (with qfabric-admin Privileges)

admin@qfabric> request component login EE3093

Warning: Permanently added 'qfabric-node-ee3093,192.0.2.0' (RSA) to the list of known hosts.
request component login (with qFabric-operator Privileges)

operator@qfabric> request component login EE3093

Warning: Permanently added 'qfabric-node-EE3093,192.0.2.0' (RSA) to the list of known hosts.

Start shell
Perform diagnostic debugging
{master}

qfabric-operator@node-ee3093>

request component login (with qfabric-user Privileges)

user0@qfabric> request component login EE3093

error: User user0 does not have sufficient permissions to login to device ee3093
request dhcp client renew

Syntax

request dhcp client renew
[all|interface <interface-name>]
routing-instance <routing-instance-name>

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Initiates a renew request for the specified clients if they are in the bound state.

Options
all—Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.

interface <interface-name>—Initiate renew requests for DHCP clients on the specified interface.

routing-instance <routing-instance-name>—Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level
view

RELATED DOCUMENTATION
 request dhcpv6 client renew | 2501

Output Fields
This command produces no output.
request dhcp server reconfigure

Syntax

```bash
request dhcp server reconfigure (all | address | interface interface-name | logical-system logical-system-name | routing-instance routing-instance-name)
```

Release Information

Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Initiate reconfiguration processing for the specified DHCP clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the `clear dhcp server binding` command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the forcerenew message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the `clear-on-abort` statement to configure the client to be cleared when reconfiguration fails.

Options

- all—Initiate reconfiguration for all DHCP clients.
- address—Initiate reconfiguration for DHCP client with the specified IP address or MAC address.
- interface interface-name—Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).

NOTE: You cannot use the `interface interface-name` option with the `request dhcp server reconfigure` command for DHCP passive clients (clients that are added as a result of DHCP snooped packets). For passive clients, the interface is not guaranteed to be the next-hop interface to the client, as is the case for active clients.

- logical-system logical-system-name—Initiate reconfiguration for all DHCP clients on the specified logical system.
**routing-instance** **routing-instance-name**—Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.

**Required Privilege Level**

view

**RELATED DOCUMENTATION**

| Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844 |

**List of Sample Output**

request dhcp server reconfigure on page 2498

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
request dhcp server reconfigure

user@host> request dhcp server reconfigure interface fe-0/0/0.100
```
request dhcpv6 server reconfigure

Syntax

request dhcpv6 server reconfigure (all | address | client-id | interface interface-name | logical-system logical-system-name | routing-instance routing-instance-name | session-id)

Release Information
Command introduced in Junos OS Release 10.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Initiate reconfiguration processing for the specified DHCPv6 clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcpv6 server binding command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfigure state and the local server sends a reconfigure message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the reconfigure message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.

Options
all—Initiate reconfiguration for all DHCPv6 clients.

address—Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.

client-id—Initiate reconfiguration for DHCPv6 client with the specified client ID.

interface interface-name—Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).

logical-system logical-system-name—Initiate reconfiguration for all DHCPv6 clients on the specified logical system.

routing-instance routing-instance-name—Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.

session-id—Initiate reconfiguration for DHCPv6 client with the specified session ID.

Required Privilege Level
view
RELATED DOCUMENTATION

Configuring Dynamic Client Reconfiguration of Extended Local Server Clients Overview | 844

List of Sample Output
request dhcpv6 server reconfigure on page 2500

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcpv6 server reconfigure

user@host> request dhcpv6 server reconfigure 2001db8::2/16
request dhcpv6 client renew

Syntax

request dhcpv6 client renew
[all | interface interface-name]
routing-instance <routing-instance-name>

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Initiate a renew request for the specified DHCPv6 clients if they are in the bound state.

Options
all—Initiate renew requests for all DHCPv6 clients. If you specify a routing instance, renew requests are initiated for all DHCPv6 clients within that routing instance.

interface-name interface-name—Initiate renew requests for DHCPv6 clients on the specified interface.

routing-instance routing-instance-name—Initiate renew requests for DHCPv6 clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level
view

Output Fields
This command produces no output.
request ipsec switch

Syntax
request ipsec switch (interface <es-fpc/pic/port> | security-associations <sa-name>)

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

Description
(Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.

Options
interface <es-fpc/pic/port>—Switch to the backup encryption interface.

security-associations <sa-name>—Switch to the backup tunnel.

Required Privilege Level
view

RELATED DOCUMENTATION
show ipsec redundancy

List of Sample Output
request ipsec switch security-associations on page 2502

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request ipsec switch security-associations
user@host> request ipsec switch security-associations sa-private
**request message**

**Syntax**

```
request message all message "text"
request message message "text" (terminal terminal-name | user user-name)
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display a message on the screens of all users who are logged in to the router or switch or on specific screens.

**Options**

- `all`—Display a message on the terminal of all users who are currently logged in.
- `message "text"`—Message to display.
- `terminal terminal-name`—Name of the terminal on which to display the message.
- `user user-name`—Name of the user to whom to direct the message.

**Required Privilege Level**

maintenance

**List of Sample Output**

`request message message on page 2503`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
user@host> request message message "Maintenance window in 10 minutes" user maria
```
Message from user@host on ttyp0 at 20:27 ...
Maintenance window in 10 minutes
EOF
request security certificate enroll (Signed)

Syntax

request security certificate enroll filename filename subject subject
alternative-subject alternative-subject certification-authority certification-authority encoding (binary | pem) key-file
  key-file  domain-name domain-name

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

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the /var/etc/ikecert directory.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard. The request security key-pair command is deprecated and not available with Junos in FIPS mode because it generates RSA and DSA keys with sizes of 512 and 1024 bits that are not compliant with the NIST SP 800-131A standard.

Options
filename filename—File that stores the certificate.
subject subject—Distinguished name (dn), which consists of a set of components—for example, an organization (o), an organization unit (ou), a country (c), and a locality (l).
alternative-subject alternative-subject—Tunnel source address.
certification-authority certification-authority—Name of the certificate authority profile in the configuration.
encoding (binary | pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.
key-file key-file—File containing a local private key.
domain-name domain-name—Fully qualified domain name.

Required Privilege Level
maintenance
List of Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed) on page 2506

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed)

user@host> request security certificate enroll filename host.crt subject c=uk,o=london alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name host.example.com

CA name: example.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.com
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check the key management process (kmd) log file at /var/log/kmd. <----------
request security certificate enroll (Unsigned)

Syntax

```
request security certificate enroll filename filename ca-file ca-file ca-name ca-name
encoding (binary | perm) url url
```

Release Information

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

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the `/var/etc/ikecert` directory.

Options

`filename filename`—File that stores the public key certificate.

`ca-file ca-file`—Name of the certificate authority profile in the configuration.

`ca-name ca-name`—Name of the certificate authority.

`encoding (binary | pem)`—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is `binary`.

`url url`—Certificate authority URL.

Required Privilege Level

maintenance

List of Sample Output

`request security certificate enroll filename ca-file ca-name url (Unsigned) on page 2507`

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
request security certificate enroll filename ca-file ca-name url (Unsigned)
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name example.com urlxyzcompany URL
```
http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: example.com
CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check the key management process (kmd) log file at /var/log/kmd.
request security key-pair

Syntax

request security key-pair filename
<size key-size>
<type (rsa | dsa)>

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

Description
(Encryption interface on M Series and T Series routers and EX Series switches only) Generate a public and private key pair for a digital certificate.

NOTE: The request security-certificates command is deprecated and are not available with Junos in FIPS mode because security certificates are not compliant with the NIST SP 800-131A standard.

Options
filename—Name of a file in which to store the key pair.

size key-size—(Optional) Key size, in bits. The key size can be 512, 1024, or 2048. The default value is 1024.

type—(Optional) Algorithm used to encrypt the key:

  • rsa—RSA algorithm. This is the default.
  • dsa—Digital signature algorithm with Secure Hash Algorithm (SHA).

Required Privilege Level
maintenance

List of Sample Output
request security key-pair on page 2510

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

request security key-pair

user@host> request security key-pair security-key-file
request security pki generate-key-pair

Syntax

request security pki generate-key-pair certificate-id certificate-id-name
<size (512 | 1024 | 2048)>
<type (dsa | rsa)>

Release Information
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description
Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate.

Options
certificate-id certificate-id-name—Name of the local digital certificate and the public/private key pair.

size—(Optional) Key pair size. The key pair size can be 512, 1024, or 2048 bits. If a key pair size is not specified, the default value, 1024 bits, is applied.

type—(Optional) The algorithm to be used for encrypting the public/private key pair. The encryption algorithm can be dsa or rsa. If an encryption algorithm is not specified, the default value, rsa, is applied.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

| Manually Generating Self-Signed Certificates on Switches (CLI Procedure) | 345 |

List of Sample Output
request security pki generate-key-pair on page 2511

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

user@switch> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
request security pki local-certificate
generate-self-signed

Syntax

```
request security pki local-certificate generate-self-signed certificate-id certificate-id-name domain-name domain-name
           ip-address ip-address email email-address subject subject-distinguished-name
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id certificate-id-name—Name of the local digital certificate and the public/private key pair.

domain-name domain-name—Fully qualified domain name (FQDN). The FQDN provides the identity of
       the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the
       subject name.

email email-address—E-mail address of the certificate holder.

ip-address ip-address—IP address of the switch.

subject subject-distinguished-name—Distinguished name format that contains the common name,
       department, company name, state, and country:

- CN—Common name
- OU—Organizational unit name
- O—Organization name
- ST—State
- C—Country

Required Privilege Level

maintenance
security

RELATED DOCUMENTATION
Manually Generating Self-Signed Certificates on Switches (CLI Procedure) | 345

List of Sample Output
request security pki local-certificate generate-self-signed on page 2514

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate generate-self-signed
user@switch> request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name abc.net email jdoe@abc.net

Self-signed certificate generated and loaded successfully
request security ssh key-pair-identity generate

Syntax

request security ssh key-pair-identity generate <identity-name> passphrase passphrase

Release Information
Command introduced in Junos OS Release 15.1X49-D70.

Description
Generate the SSH private and public key pair for a specified identity. The private and public key files are stored in the /var/db directory, which is accessible through root only. Filenames are based on the identity-name with extensions. The files are similar to the certificate files that are stored in Junos OS.

Options
• identity-name—Identity name.
• passphrase passphrase—An SSH identity generated with a passphrase. The passphrase is used to protect the private key file stored in the file system. This option does not allow the user to enter a weak passphrase, which ensures stronger security. A private key is used to connect to a remote server and is never displayed or transferred between servers, even if the system is compromised. The private key cannot be used to connect to a remote server if the passphrase is not known.

NOTE: By default, the passphrase uses Advanced Encryption Standard (AES) 128 in cipher block chaining (CBC) mode to encrypt a private key. All generated keys are stored in the /var/db/ssh_key directory.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

show security ssh key-pair-identity | 2776
clear security ssh key-pair-identity | 2488

List of Sample Output
request security ssh key-pair-identity with passphrase on page 2516

Output Fields
When you enter this command, you are provided feedback on the status of your request.

### Sample Output

```bash
request security ssh key-pair-identity with passphrase
user@host> request security ssh key-pair-identity generate myident passphrase 1q2w3e
```

```
Created SSH key myident
```
request security tpm master-encryption-password set

Syntax

request security tpm master-encryption-password set plain-text-password

Release Information
Command introduced in Junos OS Release 15.1X49-D80.

Description
Use this command to set or replace the password (in plain text).

Options
plain-text-password—Set or replace the password (in plain text).

Required Privilege Level
maintenance

RELATED DOCUMENTATION

show security tpm status | 2782

List of Sample Output
show security tpm status on page 2517

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

show security tpm status

user@host> request security tpm master-encryption-password set plain-text-password

Enter new master encryption password:
Repeat new master encryption password:
Binding password with TPM
Master encryption password is bound to TPM
Encoding master password ..
Successfully encoded master password
Encrypted key-pair files
**request system autorecovery state**

**Syntax**

```
request system autorecovery state (save | recover | clear)
```

**Release Information**
Command introduced in Junos OS Release 15.1X49-D35 for SRX300, SRX320, SRX345, and SRX550M devices.

**Description**
Prepare the system for autorecovery of configuration, licenses, and disk information.

**Options**
- **save**—Save the current state of the disk partitioning, configuration, and licenses for autorecovery.
  
The active Junos OS configuration is saved as the Junos rescue configuration, after which the rescue configuration, licenses, and disk partitioning information is saved for autorecovery. Autorecovery information must be initially saved using this command for the autorecovery feature to verify integrity of data on every bootup.

  **NOTE:**
  - Any recovery performed at a later stage will restore the data to the same state as it was when the save command was executed.
  - A fresh rescue configuration is generated when the command is executed. Any existing rescue configuration will be overwritten.

- **recover**—Recover the disk partitioning, configuration, and licenses.
  
  After autorecovery data has been saved, the integrity of saved items is always checked automatically on every bootup. The recovery command allows you to forcibly re-run the tests at any time if required.

- **clear**—Clear all saved autorecovery information.
  
  Only the autorecovery information is deleted; the original copies of the data used by the router are not affected. Clearing the autorecovery information also disables all autorecovery integrity checks performed during bootup.

**Required Privilege Level**
maintenance
RELATED DOCUMENTATION

show system autorecovery state | 2854

List of Sample Output
request system autorecovery state save on page 2520
request system autorecovery state recover on page 2520
request system autorecovery state clear on page 2521

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system autorecovery state save

user@host> request system autorecovery state save

Saving config recovery information
Saving license recovery information
Saving bsdlabel recovery information

Sample Output

request system autorecovery state recover

user@host> request system autorecovery state recover

<table>
<thead>
<tr>
<th>Configuration:</th>
<th>Recovery Information</th>
<th>Integrity Check</th>
<th>Action / Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rescue.conf.gz</td>
<td>Saved</td>
<td>Passed</td>
<td>None</td>
</tr>
<tr>
<td>Licenses:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JUNOS282736.lic</td>
<td>Saved</td>
<td>Passed</td>
<td>None</td>
</tr>
<tr>
<td>JUNOS282737.lic</td>
<td>Saved</td>
<td>Failed</td>
<td>Recovered</td>
</tr>
<tr>
<td>BSD Labels:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s1</td>
<td>Saved</td>
<td>Passed</td>
<td>None</td>
</tr>
<tr>
<td>s2</td>
<td>Saved</td>
<td>Passed</td>
<td>None</td>
</tr>
<tr>
<td>s3</td>
<td>Saved</td>
<td>Passed</td>
<td>None</td>
</tr>
</tbody>
</table>
Sample Output

request system autorecovery state clear

user@host> request system autorecovery state clear

Clearing config recovery information
    Clearing license recovery information
    Clearing bsdlabel recovery information
request system decrypt password

Syntax

request system decrypt password

Release Information

Statement introduced in Junos OS Release 15.1X49-D50 for SRX Series devices.

Description

Use to display plain text versions of obfuscated ($9) or encrypted ($8) passwords. If the password was encrypted using the new $8$ method, you are prompted for the master password.

Options

- **decrypt**—Decrypt a $8$-encrypted or $9$-encrypted password.

Required Privilege Level

system

RELATED DOCUMENTATION

- master-password | 1936
- Hardening Shared Secrets in Junos OS | 200

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

// Decrypting a $9 password
user@host> request system decrypt password $9$ABC123
Plaintext password: mysecret
Sample Output

```plaintext
// Decrypting a $8 password
user@host> request system decrypt password $8$ABC123
Master password:
Plaintext password: mysecret
(Simple passwords like “mysecret” are discouraged. This is an example only.)
```
request system download abort

Syntax

request system download abort <download-id>

Release Information

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description

Abort a download. The download instance is stopped and cannot be resumed. Any partially downloaded file is automatically deleted to free disk space. Information regarding the download is retained and can be displayed with the `show system download` command until a `request system download clear` operation is performed.

NOTE: Only downloads in the active, paused, and error states can be aborted.

Options

download-id—(Required) The ID number of the download to be aborted.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

- request system download start | 2531
- request system download pause | 2527
- request system download resume | 2529
- request system download clear | 2526

List of Sample Output
request system download abort on page 2525

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system download abort

user@host>  request system download abort 1

Aborted download #1
request system download clear

Syntax

```
request system download clear
```

Release Information
Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description
Delete the history of completed and aborted downloads.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>request system download start</td>
<td>2531</td>
</tr>
<tr>
<td>request system download pause</td>
<td>2527</td>
</tr>
<tr>
<td>request system download resume</td>
<td>2529</td>
</tr>
<tr>
<td>request system download abort</td>
<td>2524</td>
</tr>
</tbody>
</table>

List of Sample Output
request system download clear on page 2526

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request system download clear

Cleared information on completed and aborted downloads
```
request system download pause

Syntax

```
request system download pause <download-id>
```

**Release Information**

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

**Description**

Suspend a particular download instance.

**NOTE:** Only downloads in the active state can be paused.

**Options**

`download-id`—(Required) The ID number of the download to be paused.

**Required Privilege Level**

maintenance

**RELATED DOCUMENTATION**

- `request system download start` | 2531
- `request system download resume` | 2529
- `request system download abort` | 2524
- `request system download clear` | 2526

**List of Sample Output**

- `request system download pause on page 2528`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system download pause

user@host> request system download pause 1

Paused download #1
request system download resume

Syntax

request system download resume download-id <max-rate>

Release Information
Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description
Resume a download that has been paused. Download instances that are not in progress because of an error or that have been explicitly paused by the user can be resumed by the user. The file will continue downloading from the point where it paused. By default, the download resumes with the same bandwidth specified with the request system download start command. The user can optionally specify a new (maximum) bandwidth with the request system download resume command.

NOTE: Only downloads in the paused and error states can be resumed.

Options
download-id—(Required) The ID number of the download to be resumed.
max-rate—(Optional) The maximum bandwidth for the download.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

- request system download start | 2531
- request system download pause | 2527
- request system download abort | 2524
- request system download clear | 2526

List of Sample Output
request system download resume on page 2530
Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
request system download resume
user@host> request system download resume 1

Resumed download #1
```
request system download start

Syntax

```
request system download start (sftp-url | delay | identity-file | login | max-rate | passphrase | save-as)
```

Release Information
Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.
Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.

Description
Create a download instance and identify it with a unique integer called the download ID.

Options
`sftp-url`—(Required) The FTP or HTTP URL location of the file to be downloaded securely.

delay—(Optional) The number of hours after which the download should start (range from 1 through 48 hours).

`identity-file`—(Required) The name of the file requesting a Secure FTP (SFTP) download. The SFTP in smart download leverages public key authentication to authenticate a download request. Users need to generate a private or public key pair before starting a download, and then upload a public key to an SFTP server.

`login`—(Optional) The username and password for the server in the format `username:password`.

`max-rate`—(Optional) The maximum average bandwidth for the download. Numbers with the suffix k or K, m or M, and g or G are interpreted as Kbps, Mbps, or Gbps, respectively.

`passphrase`—(Required) The passphrase to protect the private key file stored on the file system. This option does not allow the user to enter a weak passphrase, which ensures stronger security.

`save-as`—(Optional) The filenameto be used for saving the file in the `/var/tmp` location.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

- request system download pause | 2527
- request system download resume | 2529
- request system download abort | 2524
List of Sample Output
request system download start on page 2532

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system download start

user@host> request system download start identity-file mytestkey
sftp://mysftpserver/homes/kelly/test.tgz max-rate 200 save as newfile.tgz

Starting download #8
request system firmware upgrade

Syntax

request system firmware upgrade

Release Information
Command introduced in Junos OS Release 10.2.

Description
Upgrade firmware on a system.

Options
fpc—Upgrade FPC ROM monitor.

pic—Upgrade PIC firmware.

re—Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.

- bios—(Optional) Upgrade BIOS.
- fpga—(Optional) Upgrade baseboard FPGA.
- i40nvm—(Optional) Upgrade baseboard i40.
- ssd—(Optional) Upgrade Routing Engine solid-state drive (SSD) firmware.
  - disk1—Upgrade SSD disk1 firmware.
  - disk2—Upgrade SSD disk2 firmware.

NOTE: Starting in Junos OS Release 17.2R1, you can upgrade the SSD firmware on routers with the VM Host support.

Starting in Junos OS Release 19.3R1, you can upgrade the i40e NVM firmware on routers with VM Host support.

vcpu—Upgrade VCPU ROM monitor.

Required Privilege Level
maintenance

RELATED DOCUMENTATION
### Sample Output

#### request system firmware upgrade

```
user@host> request system firmware upgrade re bios

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Tag</th>
<th>Current</th>
<th>Available</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Engine 0 RE BIOS</td>
<td>0</td>
<td>1.5</td>
<td>1.9</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 0 RE BIOS Backup</td>
<td>1</td>
<td>1.7</td>
<td>1.9</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

Perform indicated firmware upgrade ? [yes,no] (no) yes
```

```
user@host> request system firmware upgrade re bios backup

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Tag</th>
<th>Current</th>
<th>Available</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Engine 0 RE BIOS</td>
<td>0</td>
<td>1.5</td>
<td>1.9</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 0 RE BIOS Backup</td>
<td>1</td>
<td>1.7</td>
<td>1.9</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

Perform indicated firmware upgrade ? [yes,no] (no) yes
```

```
user@host> request system firmware upgrade re ssd disk1

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Tag</th>
<th>Current</th>
<th>Available</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Engine 0 RE SSD1</td>
<td>4</td>
<td>12028</td>
<td>12029</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated, use "show system firmware" to monitor status.
```
request system license update

Syntax

request system license update

Release Information
Command introduced in Junos OS Release 9.5.

Description
Starts autoupdating license keys from the license portal.

- The `request system license update` command always uses the default Juniper license server: `https://ae1.juniper.net/`.
- The `request system license update` command is supported only on SRX, vSRX, and QFX Series devices.

The products supported by the Juniper Agile Licensing (JAL) portal includes: QFX series, SRX Series, EX Series, NFX, vBNG, vMX, vSRX, and ACX. For other Juniper products (SPACE, JSA, SBR Carrier, Screen OS and so on) access the License Management System (LMS).

Options

- trial—Immediately updates trial license keys from the license portal.

Required Privilege Level
maintenance

List of Sample Output

- `request system license update` on page 2535
- `request system license update trial` on page 2536

Output Fields
When you enter this command, you are provided feedback on the status of your request.

---

Sample Output

```
user@host> request system license update
Trying to update license keys from https://ae1.juniper.net has been sent, use show system license to check status.
```
request system license update trial

user@host> request system license update trial

Request to automatically update trial license keys from https://ae1.juniper.net has been sent, use show system license to check status.
request system reboot

List of Syntax
Syntax on page 2537
Syntax (EX Series Switches and EX Series Virtual Chassis) on page 2537
Syntax (MX Series Routers and MX Series Virtual Chassis, EX9200 Switches and EX9200 Virtual Chassis) on page 2537
Syntax (QFabric Systems) on page 2538
Syntax (QFX Series Switches and QFX Series Virtual Chassis, Virtual Chassis Fabric) on page 2538
Syntax (TX Matrix Router) on page 2538
Syntax (TX Matrix Plus Router) on page 2538

Syntax

```
request system reboot
  <at time>
  <both-routing-engines>
  <in minutes>
  <media (compact-flash | disk | removable-compact-flash | usb)>
  <message "text">
  <other-routing-engine>
```

Syntax (EX Series Switches and EX Series Virtual Chassis)

```
request system reboot
  <all-members | local | member member-id>
  <at time>
  <in minutes>
  <media (external | internal)> | <media (compact-flash | disk | removable-compact-flash | usb)>
  <message "text">
  <slice slice>
```

Syntax (MX Series Routers and MX Series Virtual Chassis, EX9200 Switches and EX9200 Virtual Chassis)

```
request system reboot
  <all-members | local | member member-id>
  <at time>
  <both-routing-engines>
  <in minutes>
  <media (external | internal)> | <media (compact-flash | disk | usb)> | <junos | network | oam | usb>
  <message "text">
  <other-routing-engine>
```
Syntax (QFabric Systems)

request system reboot
<all <graceful>>
<at time>
<director-device name>
<director-group <graceful>>
<fabric <graceful>>
<in minutes>
<in-service>
<media>
<message “text”>
<node-group name>
<slice slice>

Syntax (QFX Series Switches and QFX Series Virtual Chassis, Virtual Chassis Fabric)

request system reboot
<all-members | local | member member-id>
<at time>
<in minutes>
<in-service>
<hypervisor>
<junos | network | oam | usb>
<message “text”>
<slice slice>

Syntax (TX Matrix Router)

request system reboot
<all-chassis | all-lcc | lcc number | scc>
<at time>
<both-routing-engines>
<in minutes>
<media (compact-flash | disk)>
<message “text”>
<other-routing-engine>

Syntax (TX Matrix Plus Router)

request system reboot
<all-chassis | all-lcc | lcc number | sfc number>
<at time>
Release Information
Command introduced before Junos OS Release 7.4.
Option other-routing-engine introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option partition changed to slice in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option both-routing-engines introduced in Junos OS Release 12.1.

Description
Reboot the software.

This command can be used on standalone devices and on devices supported in a Virtual Chassis, Virtual Chassis Fabric, or QFabric system.

NOTE: Starting with Junos OS Release 15.1F3, the statement request system reboot reboots only the guest operating system on the PTX5000 with RE-PTX-X8-64G and, MX240, MX480, and MX960 with RE-S-X6-64G.

Starting with Junos OS Release 15.1F5, the statement request system reboot reboots only the guest operating system on the MX2010, and MX2020 with REMX2K-X8-64G.

NOTE: Starting from Junos OS Release 17.2R1, PTX10008 routers do not support the request system reboot command. Starting from Junos OS Release 17.4R1, PTX10016 routers do not support the request system reboot command. Use the request vmhost reboot command instead of the request system reboot command on the PTX10008 and PTX10016 routers to reboot the Junos OS software package or bundle on the router. See request vmhost reboot.

NOTE: On a QFabric system, to avoid traffic loss on the network Node group, switch mastership of the Routing Engine to the backup Routing Engine, and then reboot.
Options
The options described here are not all supported on every platform or release of Junos OS. Refer to the Syntax sections for the options commonly available on each type of platform.

none—Reboot the software immediately.

all-chassis—(Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members | local | member member-id—(Optional) Specify which member of the Virtual Chassis to reboot:

- all-members—Reboots each switch that is a member of the Virtual Chassis.
- local—Reboots only the local switch (switch where you are logged in).
- member member-id—Reboots the specified member switch of the Virtual Chassis

at time—(Optional) Time at which to reboot the software, specified in one of the following ways:

- now—Stop or reboot the software immediately. This is the default.
- +minutes—Number of minutes from now to reboot the software.
- yymmdhhmm—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- hh:mm—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

hypervisor—(Optional) Reboot Junos OS, host OS, and any installed guest VMs.

in minutes—(Optional) Number of minutes from now to reboot the software. The minimum value is 1. This option is an alias for the at +minutes option.

in-service—(Optional) Enables you to reset the software state (no software version change) of the system with minimal disruption in data and control traffic.

junos—(Optional) Reboot from the Junos OS (main) volume.

lcc number—(Optional) Line-card chassis (LLC) number.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**media** *(compact-flash | disk | removable-compact-flash | usb)*—(Optional) Use the indicated boot medium for the next boot.

**media** *(external | internal)*—(Optional) Use the indicated boot medium for the next boot:

• **external**—Reboot the device using a software package stored on an external boot source, such as a USB flash drive.

• **internal**—Reboot the device using a software package stored in an internal memory source.

**message** "text"—(Optional) Message to display to all system users before stopping or rebooting the software.

**network**—(Optional) Reboot using the Preboot Execution Environment (PXE) boot method over the network.

**oam**—(Optional) Reboot from the maintenance volume (OAM volume, usually the compact flash drive).

**other-routing-engine**—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

**partition** **partition**—(Optional) Reboot using the specified partition on the boot media. This option is equivalent to the **slice** option that is supported on some devices. Specify one of the following **partition** values:

• **1**—Reboot from partition 1.

• **2**—Reboot from partition 2.

• **alternate**—Reboot from the alternate partition.

**scc**—(Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

**sfc number**—(Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace **number** with 0.

**slice** **slice**—(Optional) Reboot using the specified partition on the boot media. This option was originally the **partition** option but was renamed to **slice** on EX Series and QFX Series switches. Specify one of the following **slice** values:
• 1—Reboot from partition 1.
• 2—Reboot from partition 2.
• alternate—Reboot from the alternate partition (which did not boot the switch at the last bootup).

**NOTE:** The slice option is not supported on QFX Series switches that have no alternate slice when Junos OS boots as a Virtual Machine (VM). To switch to the previous version of Junos OS, issue the `request system software rollback` command.

`usb`—(Optional) Reboot from a USB device.

The following options are available only on QFabric Systems:

all—(Optional) Reboots the software on the Director group, fabric control Routing Engines, fabric manager Routing Engines, Interconnect devices, and network and server Node groups.

director-device name—(Optional) Reboots the software on the Director device and the default partition (QFabric CLI).

director-group—(Optional) Reboots the software on the Director group and the default partition (QFabric CLI).


node-group name—(Optional) Reboots the software on a server Node group or a network Node group.

graceful—(Optional) Enables the QFabric component to reboot with minimal impact to network traffic.

This sub-option is only available for the all, fabric, and director-group options.

**Additional Information**

Reboot requests are recorded in the system log files, which you can view with the `show log` command (see `show log`). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the `show system processes` command (see `show system processes`).

On a TX Matrix or TX Matrix Plus router, if you issue the `request system reboot` command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.
NOTE: Before issuing the `request system reboot` command on a TX Matrix Plus router with no options or the `all-chassis`, `all-lcc`, `lcc number`, or `sfc` options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the `request system reboot` command.

NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

**Required Privilege Level**

maintenance

**RELATED DOCUMENTATION**

- `clear system reboot`
- `request system halt`
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*
- `request vmhost reboot`

**List of Sample Output**

- `request system reboot` on page 2544
- `request system reboot (at 2300)` on page 2544
- `request system reboot (in 2 Hours)` on page 2544
- `request system reboot (Immediately)` on page 2544
- `request system reboot (at 1:20 AM)` on page 2544
- `request system reboot in-service` on page 2545

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system reboot

user@host> request system reboot

Reboot the system? [yes,no] (no)

request system reboot (at 2300)

user@host> request system reboot at 2300 message ?Maintenance time!?

Reboot the system? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@test.example.net ***
System going down at 23:00

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (Immediately)

user@host> request system reboot at now

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120

request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
request system reboot in-service

user@switch> request system reboot in-service

Reboot the system? [yes,no]

[Feb 22 02:37:04]: ISSU: Validating Image

PRE ISSR CHECK:
---------------
PFE Status: Online
Member Id zero: Valid
VC not in mixed or fabric mode: Valid
Member is single node vc: Valid
BFD minimum-interval check done: Valid
GRES enabled: Valid
NSR enabled: Valid
drop-all-tcp not configured: Valid
Ready for ISSR: Valid

warning: Do NOT use /user during ISSR. Changes to /user during ISSR may get lost!

Current image is jinstall-jcp-i386-flex-18.1.img

[Feb 22 02:37:14]: ISSU: Preparing Backup RE
Prepare for ISSR
[Feb 22 02:37:19]: ISSU: Backup RE Prepare Done
Spawning the backup RE
Spawn backup RE, index 1 successful
Starting secondary dataplane
Second dataplane container started
GRES in progress
Waiting for backup RE switchover ready
GRES operational

Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade for ISSR
Chassis ISSU Started
[Feb 22 02:42:55]: ISSU: Preparing Daemons
[Feb 22 02:43:00]: ISSU: Daemons Ready for ISSU
[Feb 22 02:43:05]: ISSU: Starting Upgrade for FRUs
[Feb 22 02:43:15]: ISSU: FPC Warm Booting
[Feb 22 02:44:16]: ISSU: FPC Warm Booted
[Feb 22 02:44:27]: ISSU: Preparing for Switchover
[Feb 22 02:44:31]:ISSU: Ready for Switchover
Checking In-Service-Upgrade status

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>Online (ISSU)</td>
<td></td>
</tr>
</tbody>
</table>

Send ISSR done to chassisd on backup RE

Chassis ISSU Completed

Removing dcpfe0 eth1 128.168.0.16 IP

Bringing down bme00

Post Chassis ISSU processing done

[Feb 22 02:44:33]:ISSU: IDLE

Stopping primary dataplane

Clearing ISSU states

Console and management sessions will be disconnected. Please login again.

device_handoff successful ret: 0

Shutdown NOW!

[pid 14305]

*** FINAL System shutdown message from root@sw-duckhorn-01 ***

System going down IMMEDIATELY
request system reboot (SRX Series)

Syntax

request system reboot <at time> <in minutes> <media> <message "text">

Release Information
Command introduced in Junos OS Release 10.1.
Command hypervisor option introduced in Junos OS Release 15.1X49-D10 for vSRX.
Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.

Description
Reboot the software.

Options
• at time (Optional)— Specify the time at which to reboot the device. You can specify time in one of the following ways:
  • now— Reboot the device immediately. This is the default.
  • +minutes— Reboot the device in the number of minutes from now that you specify.
  • yymmddhhmm— Reboot the device at the absolute time on the date you specify. Enter the year, month, day, hour (in 24-hour format), and minute.
  • hh:mm— Reboot the device at the absolute time you specify, on the current day. Enter the time in 24-hour format, using a colon (:) to separate hours from minutes.
• in minutes (Optional)— Specify the number of minutes from now to reboot the device. This option is a synonym for the at +minutes option
• media type (Optional)— Specify the boot device to boot the device from:
  • disk/internal— Reboot from the internal media. This is the default.
  • usb— Reboot from the USB storage device.
  • compact flash— Reboot from the external CompactFlash card.

NOTE: The media command option is not available on vSRX.

• message “text” (Optional)— Provide a message to display to all system users before the device reboots.
Example: request system reboot at 5 in 50 media internal message stop

Required Privilege Level
maintenance

RELATED DOCUMENTATION

request system software rollback (SRX Series) | 2557
**request system services dhcp**

**Syntax**

```
request system services dhcp (release interface-name | renew interface-name)
```

**Release Information**

Command introduced in Junos OS Release 8.5.

**Description**

Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the `show system services dhcp client interface-name` command.

**Options**

- **release interface-name** — Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.

- **renew interface-name** — Reacquires an IP address from the server for the interface. When you use this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.

**Required Privilege Level**

maintenance

**RELATED DOCUMENTATION**

<table>
<thead>
<tr>
<th>dhcp</th>
</tr>
</thead>
<tbody>
<tr>
<td>show system services dhcp client</td>
</tr>
</tbody>
</table>

**Output Fields**

This command produces no output.
request system snapshot (Maintenance)

Syntax

request system snapshot
<config-partition>
<media (compact-flash | hard-disk | internal | usb)>
<partition>
<root-partition>
<factory>
<node (all | local | node-id | primary)>
<slice (alternate)>

Release Information
Command introduced in Junos OS Release 10.2.

Description
Back up the currently running and active file system partitions on the device.

Options

- **config-partition**— Creates a snapshot of the configuration partition only and stores it onto the default /altconfig on the hard disk device or an /altconfig on a USB device.

- **root-partition**— Creates a snapshot of the root partition only and stores it onto the default /altroot on the hard disk device or an /altroot on a USB device.

- **factory**— (Optional) Specifies that only the files shipped from the factory are included in the snapshot.

- **media**— (Optional) Specify the boot device the software is copied to:
  - **compact-flash**— Copy software to the primary compact flash drive.
  - **hard-disk**— Copy software to the hard disk.
  - **usb**— Copy software to the device connected to the USB port.
  - **internal**— Copy software to an internal flash drive. This is the default option.

  **NOTE:** USB option is available on all SRX series devices; hard disk and compact-flash options are available only on SRX5800, SRX5600, and SRX5400 devices; media internal option is available only on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

- **external**— Copies software to an external storage device. This option is available for the compact flash on the SRX650 Services Gateway.
- **node**—(Optional) Specify the archive data and executable areas of a specific node. If you do not specify the node option, the device considers the current node as default option.
  - **node-id**—Specify for node (0, 1).
  - **all**—Specify for all nodes.
  - **local**—Specify for local nodes.
  - **primary**—Specify for primary nodes.

- **partition**—(Default) Specify that the target media should be repartitioned before the backup is saved to it.

  **NOTE:** The target media is partitioned whether or not it is specified in the command, because this is a mandatory option.

  Example: `request system snapshot media usb partition`

  Example: `request system snapshot media usb partition factory`

- **slice**—(Optional) Take a snapshot of the root partition the system has currently booted from to another slice in the same media.
  - **alternate**—(Optional) Store the snapshot on the other root partition in the system.

  **NOTE:** The slice option cannot be used along with the other `request system snapshot` options, because the options are mutually exclusive. If you use the factory, media, or partition option, you cannot use the slice option; if you use the slice option, you cannot use any of the other options.

**Required Privilege Level**

maintenance

**List of Sample Output**

- `request system snapshot config-partition on page 2552`
- `request system snapshot root-partition on page 2552`
- `request system snapshot media hard-disk on page 2552`
- `request system snapshot media usb (when usb device is missing on page 2552`
- `request system snapshot media compact-flash on page 2553`
- `request system snapshot partition on page 2553`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system snapshot config-partition
user@host> request system snapshot config-partition

Doing the initial labeling...
Verifying compatibility of destination media partitions...
Running newfs (391MB) on hard-disk media /config partition (ad1s1e)...
Copying '/dev/ad0s1e' to '/dev/ad1s1e' .. (this may take a few minutes)
The following filesystems were archived: /config

request system snapshot root-partition
user@host> request system snapshot root-partition

Doing the initial labeling...
Verifying compatibility of destination media partitions...
Running newfs (3GB) on hard-disk media / partition (ad1s1a)...
Copying '/dev/ad0s1a' to '/dev/ad1s1a' .. (this may take a few minutes)
The following filesystems were archived: /

request system snapshot media hard-disk
user@host> request system snapshot media hard-disk

Verifying compatibility of destination media partitions...
Running newfs (880MB) on hard-disk media / partition (ad2s1a)...
Running newfs (98MB) on hard-disk media /config partition (ad2s1e)...
Copying '/dev/ad0s1a' to '/dev/ad2s1a' .. (this may take a few minutes)
...

request system snapshot media usb (when usb device is missing)
user@host> request system snapshot media usb

Verifying compatibility of destination media partitions...
Running newfs (254MB) on usb media / partition (da1s1a)...
Running newfs (47MB) on usb media /config partition (da1s1e)...
Copying '/dev/da0s2a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2e' to '/dev/da1s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
request system snapshot media compact-flash

user@host> request system snapshot media compact-flash

error: cannot snapshot to current boot device

request system snapshot partition

user@host> request system snapshot partition

Verifying compatibility of destination media partitions...
Running newfs (439MB) on internal media / partition (da0s1a)...
Running newfs (46MB) on internal media /config partition (da0s1e)...
Copying '/dev/da1s1a' to '/dev/da0s1a' .. (this may take a few minutes)
Copying '/dev/da1s1e' to '/dev/da0s1e' .. (this may take a few minutes)
The following filesystems were archived: / /config
request system software abort in-service-upgrade (ICU)

Syntax

request system software abort in-service-upgrade

Release Information

Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description

Abort an in-band cluster upgrade (ICU). This command must be issued from a router session other than the one on which you issued the request system in-service-upgrade command that launched the ICU. If an ICU is in progress, this command aborts it. If the node is being upgraded, this command will cancel the upgrade. The command is also helpful in recovering the node in case of a failed ICU.

NOTE: We recommend that you use the command only when there is an issue with the ongoing session of ISSU. You may need to manually intervene to bring the system to sane state if after issuing the command the system does not recover from the abort.

Options

This command has no options.

Required Privilege Level

view

RELATED DOCUMENTATION

Upgrading Devices in a Chassis Cluster Using ICU

List of Sample Output

request system software abort in-service-upgrade on page 2555

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system software abort in-service-upgrade

user@host> request system software abort in-service-upgrade

In-Service-Upgrade aborted
request system software add (Maintenance)

Syntax

```
request system software add package-name
```

Release Information
Partition option introduced in the command in Junos OS Release 10.1.

Description
Install the new software package on the device, for example: `request system software add junos-srxsme-10.0R2-domestic.tgz no-copy no-validate partition reboot`.

Options

- **delay-restart**—Install the software package but does not restart the software process.
- **best-effort-load**—Activate a partial load and treat parsing errors as warnings instead of errors.
- **no-copy**—Install the software package but does not saves the copies of package files.
- **no-validate**—Do not check the compatibility with current configuration before installation starts.
- **partition**—Format and re-partition the media before installation.
- **reboot**—Reboot the device after installation is completed.
- **unlink**—Remove the software package after successful installation.
- **validate**—Check the compatibility with current configuration before installation starts.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

- `request system reboot (SRX Series)` | 2547
request system software rollback (SRX Series)

Syntax

request system software rollback <node-id>

Release Information
Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 15.1X49-D50 for SRX1500 devices.
Command introduced in Junos OS Release 17.4R1 for SRX4100 and SRX4200 devices.

Description
Revert to the software that was loaded at the last successful request system software add command. The upgraded FreeBSD 11.x (supported in Junos OS Release 17.4R1) Junos OS image provides an option to save a recovery image in an Operation, Administration, and Maintenance (OAM) partition, but that option will save only the Junos OS image, not the Linux image. If a user saves the Junos OS image and recovers it later, it might not be compatible with the Linux software loaded on the system.

Options
node-id—Identification number of the chassis cluster node. It can be 0 or 1.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

request system reboot (SRX Series) | 2547
Upgrading Junos OS with Upgraded FreeBSD
Release Information for Junos OS with Upgraded FreeBSD
What Is Junos OS with Upgraded FreeBSD?
request system zeroize

Syntax

request system zeroize <media>

Description

Erases all configuration information and resets all key values. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories.

The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the Junos OS CLI by typing cli at the prompt.

Options

media—(Optional) In addition to removing all configuration and log files, the media option causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and the like. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the request system zeroize media operation can take considerably more time than the request system zeroize operation. However, the critical security parameters are all removed at the beginning of the process.

NOTE: The media option is not supported on SRX5000 line devices.

Required Privilege Level

Not applicable.

RELATED DOCUMENTATION

request system reboot (SRX Series) | 2547
request system software rollback (SRX Series) | 2557

List of Sample Output

request system zeroize on page 2559
Sample Output

request system zeroize

user@host> request system zeroize

warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

warning: zeroizing re0

Loading /boot/loader Consoles: serial port
BIOS driver C: is disk0
BIOS 607kB/2087552kB available memory

FreeBSD/i386 bootstrap loader, Revision 1.1
(builder@youcompany.com, Mon Mar 28 20:49:26 UTC 2011)
Loading /boot/defaults/loader.config
/kernel text=0x837a60 data=0x46a78+0x9d44c syms=[0x4+0x8f38+0x4+0xca1ee]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
platform_early_bootinit: MAG Series Early Boot Initialization
GDB: debug ports: sio
GDB: current port: sio
KDB: debugger backends: ddb gdb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
...
output truncated
restart (Reset)

Syntax

```
restart
<application-identification | application-security | audit-process | commitd-service | chassis-control | class-of-service |
database-replication | datapath-trace-service | ddns | dhcp | dhcp-service | dynamic-flow-capture | disk-monitoring |
event-processing | ethernet-connectivity-fault-management | ethernet-link-fault-management |
extensible-subscriber-services | fpsd | firewall | firewall-authentication-service | general-authentication-service |
gracefully | gprs-process | idp-policy | immediately | interface-control | ipmi | ipsec-key-management | flow-service |
l2-learning | l2cpd-service | lacp | license-service |
lcm | logical-system-service | mib-process | mountd-service | named-service | network-security | network-security-trace |
nfsd-service | ntpd-service | pgm | pic-services-logging | profilerd | pki-service | remote-operations | rest-api | routing |
sampling | sampling-route-record | scc-chassisd | secure-neighbor-discovery | security-intelligence | security-log |
services | service-deployment | simple-mail-client-service | soft | snmp | static-routed | statistics-service |
snmp | subscriber-management | subscriber-management-helper | system-log-vital | tunnel-oamd | uac-service |
user-ad-authentication | vrrp | web-management >
```

Release Information

Command introduced before Junos OS Release 9.2

Description

Restart a Junos OS process.

CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router to drop calls and interrupt transmission, resulting in possible loss of data.

Options

- application-identification—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
- application-security—(Optional) Restart the application security process.
- audit-process—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, for analyzing and tracking usage patterns, and for billing a user based upon the amount of time used or the type of services accessed.
- chassis-control—(Optional) Restart the chassis management process.
- class-of-service—(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.
• commitd-service—(Optional) Restart the committed services.
• database-replication—(Optional) Restart the database replication process.
• datapath-trace-service—(Optional) Restart the packet path tracing process.
• ddns—(Optional) Restart the dynamic domain name system, which dynamically updates IP addresses for registered domain names.
• dhcp—(Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
• dhcp-service—(Optional) Restart the Dynamic Host Configuration Protocol process.
• disk-monitoring—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.
• dynamic-flow-capture—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on PIC3 monitoring services cards.
• ethernet-connectivity-fault-management—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.
• ethernet-link-fault-management—(Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.
• event-processing—(Optional) Restart the event process (eventd).
• extensible-subscriber-services—(Optional) Restart the extensible subscriber services process.
• fipsd—(Optional) Restart the fipsd services.
• firewall—(Optional) Restart the firewall management process, which manages the firewall configuration and accepts or rejects packets that are transiting an interface on a router or switch.
• firewall-authentication-service—(Optional) Restart the firewall authentication service process.
• general-authentication-service—(Optional) Restart the general authentication process.
• gprs-process—(Optional) Restart the General Packet Radio Service (GPRS) process.
• gracefully—(Optional) Restart the software process.
• idp-policy—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.
• immediately—(Optional) Immediately restart the software process.
• interface-control—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.
• ipmi—(Optional) Restart the intelligent platform management interface process.
• ipsec-key-management—(Optional) Restart the IPsec key management process.
• jflow-service—(Optional) Restart jflow service process.
• jnu-management—(Optional) Restart jnu management process.
• jnx-wmicsd-service—(Optional) Restart jnx wmicsd service process.
• jsrp-service—(Optional) Restart the Juniper Services Redundancy Protocol (jsrdp) process, which controls chassis clustering.
• kernel-replication—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.
• lacp—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link. The LACP process allows link aggregation control instances to reach agreement on the identity of the LAG to which a link belongs, moves the link to that LAG, and enables the transmission and reception processes for the link to function in an orderly manner.
• l2cpd-service—(SRX5400, SRX5600, and SRX5800 devices only) (Optional) Restart the Layer 2 Control Protocol (L2CP) process, which enables features such as L2 protocol tunneling and nonstop bridging.
• l2-learning—(Optional) Restart the Layer 2 (L2) address flooding and learning process.
• license-service—(Optional) Restart the feature license management process.
• logical-system-service—(Optional) Restart the logical system service process.
• mib-process—(Optional) Restart the MIB version II process, which provides the router's MIB II agent.
• mountd-service—(Optional) Restart the service for Network File System (NFS) mount requests.
• named-service—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.
• network-security—(Optional) Restart the network security process.
• network-security-trace—(Optional) Restart the network security trace process.
• nfsd-service—(Optional) Restart the remote NFS server process, which provides remote file access for applications that need NFS-based transport.
• ntpd-service—(Optional) Restart the Network Time Protocol (NTP) process.
• pgm—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.
• pic-services-logging—(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.
• pki-service—(Optional) Restart the public key infrastructure (PKI) service process.
• profilerd—(Optional) Restart the profiler process.
• remote-operations—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
• rest-api—(Optional) Restart the rest api process.
• routing—(Optional) Restart the routing protocol process (rpd).
• sampling—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.
• sampling-route-record—(Optional) Restart the sampling route record process.
• scc-chassisd—(Optional) Restart the scc chassisd process.
• secure-neighbor-discovery—(Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.
• security-intelligence—(Optional) Restart security intelligence process.
• security-log—(Optional) Restart the security log process.
• service-deployment—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.
• services—(Optional) Restart a service.
• simple-mail-client-service—(Optional) Restart the simple mail client service process.
• snmp—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router’s or switch’s SNMP master agent.
• static-routed—(Optional) Restart the static routed process.
• soft—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.
• statistics-service—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.
• subscriber-management—(Optional) Restart the subscriber management process.
• subscriber-management-helper—(Optional) Restart the subscriber management helper process.
• system-log-vital—(Optional) Restart system log vital process.
• tunnel-oamd—(Optional) Restart the tunnel OAM process for L2 tunneled networks.
• uac-service—(Optional) Restart the Unified Access Control (UAC) process.
• user-ad-authentication—(Optional) Restart User ad Authentication process
• vrrp—(Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.
• web-management—(Optional) Restart the Web management process.

Required Privilege Level
reset
Related Documentation

Restart Commands Overview

List of Sample Output
restart interfaces on page 2564

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

restart interfaces
user@host> restart interfaces

interfaces process terminated
interfaces process restarted
show accounting server statistics archival-transfer

Syntax

show accounting server statistics archival-transfer

Release Information

Command introduced in Junos OS Release 19.2.

Description

Display the statistics of transfer attempted, succeeded, and failed for accounting statistics files and router configuration archives.

Options

This command has no options.

Required Privilege Level

view

Sample Output

show accounting server statistics archival-transfer

user@host> show accounting server statistics archival-transfer

<table>
<thead>
<tr>
<th>File Name</th>
<th>/var/transfer/config/*</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>scp://root@ce-bras-nvrsrv-a:/var/www/html</td>
</tr>
<tr>
<td>Last transfer attempted timestamp</td>
<td>20190603_143642</td>
</tr>
<tr>
<td>Last successful transfer timestamp</td>
<td>20190603_143642</td>
</tr>
<tr>
<td>Success Count</td>
<td>5</td>
</tr>
<tr>
<td>Failure Count</td>
<td>0</td>
</tr>
</tbody>
</table>
show captive-portal authentication-failed-users

Syntax

```
show captive-portal authentication-failed-users
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display the users that have failed captive portal authentication.

Required Privilege Level

view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>show captive-portal interface</th>
<th>2571</th>
</tr>
</thead>
<tbody>
<tr>
<td>show captive-portal firewall</td>
<td>2568</td>
</tr>
<tr>
<td>clear captive-portal</td>
<td>2452</td>
</tr>
</tbody>
</table>

Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485

Configuring Captive Portal Authentication (CLI Procedure) | 492

List of Sample Output

show captive-portal authentication-failed-users on page 2567

Output Fields

Table 63 on page 2566 lists the output fields for the `show captive-portal authentication-failed-users` command. Output fields are listed in the approximate order in which they appear.

Table 63: show captive-portal authentication-failed-users Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MAC address configured to bypass captive portal authentication.</td>
<td>all</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address configured statically on the interface.</td>
<td>all</td>
</tr>
</tbody>
</table>
Table 63: show captive-portal authentication-failed-users Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Name of the user that has failed captive portal authentication.</td>
<td>all</td>
</tr>
<tr>
<td>Failure Count</td>
<td>The number of times that 802.1X authentication has failed on the interface.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

```bash
show captive-portal authentication-failed-users

user@host> show captive-portal authentication-failed-users
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC address</th>
<th>User</th>
<th>Failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/17.0</td>
<td>00:37:00:00:00:00</td>
<td>003700000000</td>
<td>28</td>
</tr>
<tr>
<td>ge-0/0/20.0</td>
<td>00:04:10:00:00:00</td>
<td>000410000000</td>
<td>32</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>00:00:03:00:0a:00</td>
<td>000003000a00</td>
<td>4</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>00:00:03:00:0b:00</td>
<td>000003000b00</td>
<td>18</td>
</tr>
</tbody>
</table>
show captive-portal firewall

Syntax

```
show captive-portal firewall
<brief | detail>
<interface-name>
<interface-name detail>
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display information about the firewall filters for each user that is authenticated on each captive portal interface.

Options

- **none**—Display all the firewall filters on all captive portal interfaces.
- **brief | detail**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display all the terms of the firewall filters for the specified interface.
- **interface-name detail**—(Optional) Display all of the terms of the firewall filters for the specified interface.

Required Privilege Level

view

RELATED DOCUMENTATION

- show captive-portal authentication-failed-users | 2566
- show captive-portal interface | 2571
- clear captive-portal | 2452
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492

List of Sample Output

show captive-portal firewall brief on page 2569
show captive-portal firewall (Specific Interface) on page 2569
show captive-portal firewall on page 2569

Output Fields
Output fields for the `show captive-portal firewall` command include any action modifier specified in firewall filters except policers. Policers are not supported in the terms of the internally generated dynamic firewall filters that are created when multiple supplicants authenticate on 802.1X-enabled interfaces.

Sample Output

`show captive-portal firewall brief`

```
user@switch> show captive-portal firewall brief

Captive Portal Information:
Interface    State     MAC address      User
ge-0/0/1.0   Connecting   00:30:48:8c:66:bd   No User
ge-0/0/10.0  Connecting   00:30:48:8c:66:bd   No User
```

`show captive-portal firewall (Specific Interface)`

```
user@switch> show captive-portal firewall ge-0/0/10.0

Filter name: dot1x_ge-0/0/10
Counters:
Name                                  Bytes   Packets
dot1x_ge-0/0/10_CP_arp                7616     119
dot1x_ge-0/0/10_CP_dhcp                0       0
dot1x_ge-0/0/10_CP_http                0       0
dot1x_ge-0/0/10_CP_https               0       0
dot1x_ge-0/0/10_CP_t_dns               0       0
dot1x_ge-0/0/10_CP_u_dns               0       0
```

`show captive-portal firewall`

```
user@switch> show captive-portal firewall

Filter name: dot1x_ge-0/0/0
Counters:
Name                                  Bytes   Packets
dot1x_ge-0/0/0_CP_arp                  0       0
dot1x_ge-0/0/0_CP_dhcp                 0       0
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/0_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter name: dot1x_ge-0/0/1

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/1_CP_arp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter name: dot1x_ge-0/0/10

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/10_CP_arp</td>
<td>7616</td>
<td>119</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter name: dot1x_ge-0/0/11
show captive-portal interface

Syntax

```
show captive-portal interface
  <interface-name>
  detail
```

Release Information
Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description
Display the current operational state of all captive portal interfaces with the list of connected users and the configured values of captive portal attributes on the interfaces.

Options
- **none**—Display all captive portal interfaces.
- **interface-name**—(Optional) Display the state for the specified captive portal interface and lists the MAC address and user names of any clients authenticated on the interface.
- **interface-name detail**—(Optional) Display the configured values of captive portal attributes on the specified captive portal interface.

Required Privilege Level
view

RELATED DOCUMENTATION

- show captive-portal authentication-failed-users | 2566
- show captive-portal firewall | 2568
- captive-portal | 1554
- clear captive-portal | 2452
- Example: Setting Up Captive Portal Authentication on an EX Series Switch | 485
- Configuring Captive Portal Authentication (CLI Procedure) | 492

List of Sample Output
Output Fields

Table 64 on page 2572 lists the output fields for the `show captive-portal interface` command. Output fields are listed in the approximate order in which they appear.

Table 64: show captive-portal interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which captive portal has been configured.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>The state of the interface:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Authenticated—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Authenticating—The client is authenticating through the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Connecting—Switch is attempting to contact the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Initialize—The interface link is down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Held—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.</td>
<td></td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the connected client on the interface.</td>
<td>brief</td>
</tr>
<tr>
<td>User</td>
<td>Users connected to the captive portal interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Fallen back</td>
<td>Indicates when 802.1X authentication and captive portal are both enabled on an interface:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If 802.1X authentication and captive portal are both enabled, CP fallen back status is Yes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If 802.1X authentication and captive portal are not both enabled, CP fallen back status is No.</td>
<td></td>
</tr>
<tr>
<td>Supplicant mode</td>
<td>Mode used to authenticate clients—multiple, single, or single-suppliant.</td>
<td>detail</td>
</tr>
<tr>
<td>Number of retries</td>
<td>Number of times the user can attempt to submit authentication information.</td>
<td>detail</td>
</tr>
</tbody>
</table>
### Table 64: show captive-portal interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quiet period</strong></td>
<td>Time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Configured CP session timeout</strong></td>
<td>Time, in seconds, that a client can be idle before the session expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server timeout</strong></td>
<td>Time, in seconds, that an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Configured CP User-keepalive timeout</strong></td>
<td>Time, in minutes, that a captive portal authentication session is extended after the MAC aging timer expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Number of connected supplicants</strong></td>
<td>Number of users connecting through the captive portal interface. Information for each user includes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Supplicant—User name and MAC address.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Operational state—See State (above).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dynamic CP session timeout—Timeout value dynamically downloaded from the RADIUS server for this user, if any.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CP Session expiration due in—Time remaining in session.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Eapol-Block—Shows whether EAPOL block is in effect or not.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CP Session User-keepalive Expiration due in—Time, in seconds, remaining in the keep-alive period.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

**show captive-portal interface (Only Captive Portal Enabled)**

```
user@switch> show captive-portal interface

Captive Portal Information:

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>MAC address</th>
<th>User</th>
<th>Fallen back</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1.0</td>
<td>Connecting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>Connecting</td>
<td>00:30:48:8c:66:bd</td>
<td>No User</td>
<td></td>
</tr>
<tr>
<td>ge-6/0/5.0</td>
<td>Authenticated</td>
<td>00:30:48:8d:7a:9b</td>
<td>abcdeX</td>
<td>No</td>
</tr>
</tbody>
</table>
```
show captive-portal interface (802.1X Authentication and Captive Portal Enabled)

user@switch> show captive-portal interface

Captive Portal Information:

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>MAC address</th>
<th>User</th>
<th>Fallen back</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1.0</td>
<td>Connecting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>Connecting</td>
<td>00:30:48:8c:66:bd</td>
<td>No User</td>
<td></td>
</tr>
<tr>
<td>ge-6/0/5.0</td>
<td>Authenticated</td>
<td>00:30:48:8d:7a:9b</td>
<td>abcdeX</td>
<td>Yes</td>
</tr>
</tbody>
</table>

show captive-portal interface detail (Only Captive Portal Enabled)

user@switch> show captive-portal interface detail ge-6/0/5.0

Supplicant mode: Multiple  
Number of retries: 3  
Quiet period: 60 seconds  
Configured CP session timeout: 3600 seconds  
Server timeout: 15 seconds  
Configured CP User-keepalive timeout: 7 minutes  
CP fallen back: No  
Number of connected supplicants: 1  
  Supplicant: abcdeX, 00:30:48:8d:7a:9b  
  Operational state: Authenticated  
  Dynamic CP Session Timeout: 3600 seconds  
  CP Session Expiration due in: 3583 seconds  
  Eapol-Block: In Effect  
  CP session User-keepalive Expiration due in: 420 seconds

show captive-portal interface detail (802.1X Authentication and Captive Portal Enabled)

user@switch> show captive-portal interface detail ge-6/0/5.0

Supplicant mode: Multiple  
Number of retries: 3  
Quiet period: 60 seconds  
Configured CP session timeout: 3600 seconds  
Server timeout: 15 seconds  
CP fallen back: Yes  
Number of connected supplicants: 1  
  Supplicant: abcdeX, 00:30:48:8d:7a:9b  
  Operational state: Authenticated  
  Dynamic CP Session Timeout: 3600 seconds
CP Session Expiration due in: 3583 seconds
Eapol-Block: In Effect
show chassis routing-engine (View)

Syntax

```
show chassis routing-engine
```

Release Information

Command introduced in Junos OS Release 9.5.

Description

Display the Routing Engine status of the chassis cluster.

Required Privilege Level

```
view
```

RELATED DOCUMENTATION

```
cluster (Chassis)
request system snapshot (Maintenance) | 2550
```

List of Sample Output

```
show chassis routing-engine (Sample 1 - SRX550M) on page 2577
show chassis routing-engine (Sample 2 - vSRX) on page 2578
show chassis routing-engine (Sample 3- SRX5400) on page 2579
show chassis routing-engine (Sample 4- SRX4100) on page 2579
show chassis routing-engine (Sample 5- SRX1500) on page 2580
```

Output Fields

Table 65 on page 2576 lists the output fields for the `show chassis routing-engine` command. Output fields are listed in the approximate order in which they appear.

Table 65: show chassis routing-engine Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Routing Engine temperature. (Not available for vSRX deployments.)</td>
</tr>
<tr>
<td>CPU temperature</td>
<td>CPU temperature. (Not available for vSRX deployments.)</td>
</tr>
</tbody>
</table>
Table 65: show chassis routing-engine Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total memory</td>
<td>Total memory available on the system.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Starting with Junos OS Release 15.1x49-D70 and Junos OS Release 17.3R1,</td>
</tr>
<tr>
<td></td>
<td>there is a change in the method for calculating the memory utilization by a Routing</td>
</tr>
<tr>
<td></td>
<td>Engine. The inactive memory is now subtracted from the total available memory.</td>
</tr>
<tr>
<td></td>
<td>There is thus, a decrease in the reported value for used memory; as the inactive</td>
</tr>
<tr>
<td></td>
<td>memory is now considered as free.</td>
</tr>
<tr>
<td>Control plane memory</td>
<td>Memory available for the control plane.</td>
</tr>
<tr>
<td>Data plane memory</td>
<td>Memory reserved for data plane processing.</td>
</tr>
<tr>
<td>CPU utilization</td>
<td>Current CPU utilization statistics on the control plane core.</td>
</tr>
<tr>
<td>User</td>
<td>Current CPU utilization in user mode on the control plane core.</td>
</tr>
<tr>
<td>Background</td>
<td>Current CPU utilization in nice mode on the control plane core.</td>
</tr>
<tr>
<td>Kernel</td>
<td>Current CPU utilization in kernel mode on the control plane core.</td>
</tr>
<tr>
<td>Interrupt</td>
<td>Current CPU utilization in interrupt mode on the control plane core.</td>
</tr>
<tr>
<td>Idle</td>
<td>Current CPU utilization in idle mode on the control plane core.</td>
</tr>
<tr>
<td>Model</td>
<td>Routing Engine model.</td>
</tr>
<tr>
<td>Start time</td>
<td>Routing Engine start time.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time the Routing Engine has been up (running) since the last start.</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Reason for the last reboot of the Routing Engine.</td>
</tr>
<tr>
<td>Load averages</td>
<td>The average number of threads waiting in the run queue or currently executing</td>
</tr>
<tr>
<td></td>
<td>over 1-, 5-, and 15-minute periods.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show chassis routing-engine (Sample 1 - SRX550M)

user@host> show chassis routing-engine
```
## Routing Engine status:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>CPU temperature</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>Total memory</td>
<td>512 MB Max</td>
</tr>
<tr>
<td>Control plane memory</td>
<td>344 MB Max</td>
</tr>
<tr>
<td>Data plane memory</td>
<td>168 MB Max</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>8 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>4 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>88 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-SRX5500-LOWMEM</td>
</tr>
<tr>
<td>Serial ID</td>
<td>AAAP8652</td>
</tr>
<tr>
<td>Start time</td>
<td>2009-09-21 00:04:54 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>52 minutes, 47 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>0x200:chassis control reset</td>
</tr>
<tr>
<td>Load averages:</td>
<td></td>
</tr>
<tr>
<td>1 minute</td>
<td>0.12</td>
</tr>
<tr>
<td>5 minute</td>
<td>0.15</td>
</tr>
<tr>
<td>15 minute</td>
<td>0.10</td>
</tr>
</tbody>
</table>

## Sample Output

**show chassis routing-engine (Sample 2 - vSRX)**

```
user@host> show chassis routing-engine
```

## Routing Engine status:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total memory</td>
<td>1024 MB Max</td>
</tr>
<tr>
<td>Control plane memory</td>
<td>1024 MB Max</td>
</tr>
<tr>
<td>5 sec CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>2 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>4 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>6 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>88 percent</td>
</tr>
<tr>
<td>Model</td>
<td>VSRX RE</td>
</tr>
<tr>
<td>Start time</td>
<td>2015-03-03 07:04:18 UTC</td>
</tr>
<tr>
<td>Uptime</td>
<td>2 days, 11 hours, 51 minutes, 11 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown.</td>
</tr>
<tr>
<td>Load averages:</td>
<td></td>
</tr>
<tr>
<td>1 minute</td>
<td>0.07</td>
</tr>
<tr>
<td>5 minute</td>
<td>0.04</td>
</tr>
<tr>
<td>15 minute</td>
<td>0.06</td>
</tr>
</tbody>
</table>
Sample Output

show chassis routing-engine (Sample 3- SRX5400)

user@host> show chassis routing-engine

Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 31 degrees C / 87 degrees F
  CPU temperature             31 degrees C / 87 degrees F
  DRAM                      16323 MB (16384 MB installed)
  Memory utilization          10 percent
  5 sec CPU utilization:
    User                       2 percent
    Background                 0 percent
    Kernel                    12 percent
    Interrupt                  1 percent
    Idle                      85 percent
  Model                          RE-S-1800x4
  Serial ID                      9016272401
  Start time                     2019-07-08 01:17:10 PDT
  Uptime                         2 minutes, 43 seconds
  Last reboot reason             Router rebooted after a normal shutdown.
  Load averages:                 1 minute   5 minute  15 minute
                                 0.63       0.52       0.24

Sample Output

show chassis routing-engine (Sample 4- SRX4100)

user@host> show chassis routing-engine

Routing Engine status:
  Temperature                 29 degrees C / 84 degrees F
  CPU temperature             29 degrees C / 84 degrees F
  Total memory              1954 MB Max   567 MB used ( 29 percent)
  Memory utilization          24 percent
  5 sec CPU utilization:
    User                       0 percent
    Background                 0 percent
<table>
<thead>
<tr>
<th>Section</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kernel</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>100 percent</td>
</tr>
<tr>
<td>1 min CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>100 percent</td>
</tr>
<tr>
<td>5 min CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>100 percent</td>
</tr>
<tr>
<td>15 min CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>100 percent</td>
</tr>
<tr>
<td>Model</td>
<td>SRX Routing Engine</td>
</tr>
<tr>
<td>Serial ID</td>
<td>BUILTIN</td>
</tr>
<tr>
<td>Uptime</td>
<td>17 days, 5 hours, 1 minute, 52 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>0x4000:VJUNOS reboot</td>
</tr>
<tr>
<td>Load averages:</td>
<td>1 minute 5 minute 15 minute</td>
</tr>
<tr>
<td></td>
<td>0.00 0.00 0.00</td>
</tr>
</tbody>
</table>

The Total memory 64 GB is distributed between the routing engine in the form of virtual machine for the TVP platforms (SRX1500, SRX4100, SRX4200) and the rest for the packet forwarding engine (PFE). TVP has a different architecture differentiating PFE from Junos and additional API compatibility. The above mentioned devices are the only ones with this TVP architecture in SRX. The `show chassis routing-engine` command displays only the Routing Engine memory.

---

**Sample Output**

```
show chassis routing-engine (Sample 5- SRX1500)

user@host> show chassis routing-engine

Routing Engine status:
Temperature                42 degrees C / 107 degrees F
```
CPU temperature             42 degrees C / 107 degrees F
Total memory              1954 MB Max   528 MB used ( 27 percent)
Memory utilization          23 percent
5 sec CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     100 percent
1 min CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     99 percent
5 min CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     99 percent
15 min CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     96 percent
Model                          SRX Routing Engine
Serial ID                      BUILTIN
Uptime                         52 minutes, 27 seconds
Last reboot reason             0x4000:VJUNOS reboot
Load averages:                 1 minute   5 minute   15 minute
                                   0.00        0.00        0.00
show dhcp client binding

Syntax

```
show dhcp client binding
[<address> | interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary]
logical-system
tenant
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.
The logical-system and tenant options are introduced in Junos OS Release 18.4R1.

Description

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options

address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

logical-system—(Optional) Displays the DHCP binding information for DHCP clients on the specified logical system.

tenant—(Optional) Displays the DHCP binding information for DHCP clients on the specified tenant system.

Required Privilege Level

view
List of Sample Output
show dhcp client binding on page 2583

Output Fields
Table 66 on page 2583 lists the output fields for the show dhcp client binding command. Output fields are listed in the approximate order in which they appear.

Table 66: show dhcp client binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the DHCP client.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware address of the DHCP client.</td>
</tr>
<tr>
<td>Server</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which the lease expires.</td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the DHCP local server.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the request was received.</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client's IP address lease expires.</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds in which the lease expires.</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client's IP address lease started.</td>
</tr>
<tr>
<td>Vendor Identifier</td>
<td>Vendor identifier.</td>
</tr>
<tr>
<td>Server Identifier</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>IP address of the DHCP client.</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp client binding

user@host> show dhcp client binding
2 clients, (2 bound, 0 init, 0 discover, 0 renew, 0 rebind)

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>Hardware address</th>
<th>Server</th>
<th>Expires</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/1.0</td>
<td>10.1.1.89</td>
<td>00:0a:12:00:12:12</td>
<td>10.1.1.1</td>
<td>348</td>
<td>BOUND</td>
</tr>
<tr>
<td>fe-0/0/2.0</td>
<td>20.1.1.90</td>
<td>00:0a:12:00:12:34</td>
<td>20.1.1.1</td>
<td>568</td>
<td>BOUND</td>
</tr>
</tbody>
</table>

user@host> show dhcp client binding interface fe-0/0/1.0 detail

Client Interface: fe-0/0/1.0
Hardware address: 00:0a:12:00:12:12
State: BOUND
Lease Expires: 2010-09-16 14:45:41 UTC
Lease Expires in: 528 seconds
Lease Start: 2010-09-16 14:35:41 UTC
Vendor Identifier: ether
Server Identifier: 10.1.1.1
Client IP Address: 10.1.1.89
update server enabled

DHCP Options :
   Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3 ]
   Name: server-identifier, Value: 10.1.1.1
   Name: router, Value: [ 10.1.1.80 ]
   Name: domain-name, Value: example-50

user@host> show dhcp client binding 10.1.1.89

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>Hardware address</th>
<th>Server</th>
<th>Expires</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/1.0</td>
<td>10.1.1.89</td>
<td>00:0a:12:00:12:12</td>
<td>10.1.1.1</td>
<td>348</td>
<td>BOUND</td>
</tr>
</tbody>
</table>

user@host> show dhcp client binding tenant TSYS1 routing-instance R1
user@host> **show dhcp client binding detail tenant TSYS1 routing-instance R1**

Client Interface/Id: ge-0/0/3.0
  Hardware Address: 00:50:56:b0:b8:21
  State: BOUND (LOCAL_CLIENT_STATE_BOUND)
  Lease Expires: 2018-04-26 16:24:34 UTC
  Lease Expires in: 1626 seconds
  Lease Start: 2018-04-26 15:51:14 UTC
  Server Identifier: 11.11.11.1
  Client IP Address: 33.33.33.3
  Update Server No

DHCP options:
  Name: dhcp-lease-time, Value: 33 minutes, 20 seconds
  Name: server-identifier, Value: 11.11.11.1
  Name: router, Value: [33.33.33.1]
  Name: subnet-mask, Value: 255.255.255.0
show dhcp client statistics

Syntax

```
show dhcp client statistics
<routing-instance routing-instance-name >
logical-system
tenant
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10.
The logical-system and tenant option is introduced in Junos OS Release 18.4R1.

Description
Displays the DHCP client statistics.

Options
routing-instance routing-instance-name—(Optional) Display the statistics for DHCP clients on the specified routing instance.

logical-system—(Optional) Displays the DHCP statistics information for DHCP clients on the specified logical system.

tenant—(Optional) Displays the DHCP statistics information for DHCP clients on the specified tenant system.

Required Privilege Level
view

RELATED DOCUMENTATION
- clear dhcp client statistics | 2456

List of Sample Output
- show dhcp client statistics on page 2588
- show dhcp client statistics tenant TSYS1 routing-instance R1 on page 2588

Output Fields
Table 67 on page 2587 lists the output fields for the show dhcp client statistics command. Output fields are listed in the approximate order in which they appear.
Table 67: show dhcp client statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets dropped</td>
<td>Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td>Messages received</td>
<td>Number of DHCP messages received.</td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of DHCP messages sent.</td>
</tr>
</tbody>
</table>

- **BOOTREPLY**—Number of BOOTP protocol data units (PDUs) received
- **DHCPOFFER**—Number of DHCP PDUs of type OFFER received
- **DHCPACK**—Number of DHCP PDUs of type ACK received
- **DHCPNACK**—Number of DHCP PDUs of type NACK received
- **DHCPFORCERENEW**—Number of DHCP PDUs of type FORCERENEW received
- **BOOTREQUEST**—Number of BOOTP protocol data units (PDUs) transmitted
- **DHCPDECLINE**—Number of DHCP PDUs of type DECLINE transmitted
- **DHCPDISCOVER**—Number of DHCP PDUs of type DISCOVER transmitted
- **DHCPREQUEST**—Number of DHCP PDUs of type REQUEST transmitted
- **DHCPINFORM**—Number of DHCP PDUs of type INFORM transmitted
- **DHCPRELEASE**—Number of DHCP PDUs of type RELEASE transmitted
- **DHCPRENEW**—Number of DHCP PDUs of type RENEW transmitted
- **DHCPREBIND**—Number of DHCP PDUs of type REBIND transmitted
Sample Output

show dhcp client statistics
user@host> show dhcp client statistics

Packets dropped:
  Total                      0
Messages received:
  BOOTREPLY                  0
  DHCPOFFER                  0
  DHCPACK                    0
  DHCPNAK                    0
  DHCPFORCERENEW             0
Messages sent:
  BOOTREQUEST                0
  DHCPDECLINE                0
  DHCPDISCOVER               0
  DHCPREQUEST                0
  DHCPINFORM                 0
  DHCPRELEASE                0
  DHCPRENEW                  0
  DHCPREBIND                 0

show dhcp client statistics tenant TSYS1 routing-instance R1
user@host> show dhcp client statistics tenant TSYS1 routing-instance R1

Packets dropped:
  Total                      0
Messages received:
  BOOTREPLY                  14
  DHCPOFFER                  4
  DHCPACK                    10
  DHCPNAK                    0
  DHCPFORCERENEW             0
Messages sent:
  BOOTREQUEST                17
  DHCPDECLINE                0
  DHCPDISCOVER               4
  DHCPREQUEST                10
  DHCPINFORM                 0
<table>
<thead>
<tr>
<th>DHCP Command</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPRELEASE</td>
<td>3</td>
</tr>
<tr>
<td>DHCPRENEW</td>
<td>6</td>
</tr>
<tr>
<td>DHCPREBIND</td>
<td>0</td>
</tr>
</tbody>
</table>
show dhcp relay binding

Syntax

Show dhcp relay binding
[<address> |interface <interface-name>]
 routing-instance <routing-instance name>
 [brief | detail | summary]

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay client table.

Options
address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- ip-address—The specified IP address.
- mac-address—The specified MAC address.

routing-instance <routing-instance name>—(Optional) Display DHCP binding information on the specified routing instance.

interface <interface-name>—(Optional) Perform this operation on the specified interface.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level
view

RELATED DOCUMENTATION

| clear dhcp relay binding | 2457 |

List of Sample Output
show dhcp relay binding on page 2591
Output Fields

Table 68 on page 2591 lists the output fields for the `show dhcp relay binding` command. Output fields are listed in the approximate order in which they appear.

Table 68: show dhcp relay binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the DHCP client.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware address of the DHCP client.</td>
</tr>
<tr>
<td>Request received on</td>
<td>Interface on which the request was received.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of DHCP packet processing performed on the device.</td>
</tr>
<tr>
<td>Obtained at</td>
<td>Date and time at which the client’s IP address lease started.</td>
</tr>
<tr>
<td>Expires at</td>
<td>Date and time at which the client’s IP address lease expires.</td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the DHCP local server.</td>
</tr>
</tbody>
</table>

Sample Output

```
show dhcp relay binding
user@host>  show dhcp relay binding detail

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
<th>Type</th>
<th>Lease expires</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.20.32.1</td>
<td>90:00:00:01:00:01</td>
<td>active</td>
<td>2007-01-17 11:38:47 PST</td>
<td>rebind</td>
</tr>
<tr>
<td>100.20.32.3</td>
<td>90:00:00:02:00:01</td>
<td>active</td>
<td>2007-01-17 11:38:41 PST</td>
<td>rebind</td>
</tr>
<tr>
<td>100.20.32.4</td>
<td>90:00:00:03:00:01</td>
<td>active</td>
<td>2007-01-17 11:38:01 PST</td>
<td>rebind</td>
</tr>
<tr>
<td>100.20.32.5</td>
<td>90:00:00:04:00:01</td>
<td>active</td>
<td>2007-01-17 11:38:07 PST</td>
<td>rebind</td>
</tr>
<tr>
<td>100.20.32.6</td>
<td>90:00:00:05:00:01</td>
<td>active</td>
<td>2007-01-17 11:38:47 PST</td>
<td>rebind</td>
</tr>
</tbody>
</table>

user@host>  show dhcp relay binding 100.20.32.1
```
Active binding information:
   IP address              100.20.32.1
   Hardware address        90:00:00:01:00:01

Lease information:
   Type                 DHCP
   Obtained at          2007-01-17 11:28:47 PST
   Expires at           2007-01-17 11:38:47 PST

> show dhcp relay binding 100.20.32.1 detail
Active binding information:
   IP address              100.20.32.1
   Hardware address        90:00:00:01:00:01
   Request received on     fe-0/0/2.0, relayed by 100.20.32.2

Lease information:
   Type                 DHCP
   Obtained at          2007-01-17 11:28:47 PST
   Expires at           2007-01-17 11:38:47 PST
   State                rebind
show dhcp relay statistics

Syntax

```
show dhcp relay statistics
[<routing-instance>]
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Display Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options
`routing-instance`—(Optional) Display the DHCP relay statistics on the specified routing instance.

Required Privilege Level
view

RELATED DOCUMENTATION

| clear dhcp relay statistics | 2458 |

List of Sample Output
show dhcp relay statistics on page 2594

Output Fields
Table 69 on page 2594 lists the output fields for the `show dhcp relay statistics` command. Output fields are listed in the approximate order in which they appear.
### Table 69: show dhcp relay statistics

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages received</td>
<td>Number of DHCP messages sent.</td>
</tr>
<tr>
<td>• BOOTREQUEST</td>
<td>Number of BOOTP protocol data units (PDUs) received</td>
</tr>
<tr>
<td>• DHCPDECLINE</td>
<td>Number of DHCP PDUs of type DECLINE received</td>
</tr>
<tr>
<td>• DHCPDISCOVER</td>
<td>Number of DHCP PDUs of type DISCOVER received</td>
</tr>
<tr>
<td>• DHCPREQUEST</td>
<td>Number of DHCP PDUs of type REQUEST received</td>
</tr>
<tr>
<td>• DHCPINFORM</td>
<td>Number of DHCP PDUs of type INFORM received</td>
</tr>
<tr>
<td>• DHCPRELEASE</td>
<td>Number of DHCP PDUs of type RELEASE received</td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of DHCP messages received.</td>
</tr>
<tr>
<td>• BOOTREPLY</td>
<td>Number of BOOTP PDUs transmitted</td>
</tr>
<tr>
<td>• DHCPOFFER</td>
<td>Number of DHCP PDUs of type OFFER transmitted</td>
</tr>
<tr>
<td>• DHCPACK</td>
<td>Number of DHCP PDUs of type ACK transmitted</td>
</tr>
<tr>
<td>• DHCPNACK</td>
<td>Number of DHCP PDUs of type NACK transmitted</td>
</tr>
<tr>
<td>• DHCPFORCERENEW</td>
<td>Number of DHCP PDUs of type FORCERENEW transmitted</td>
</tr>
</tbody>
</table>

### Sample Output

**show dhcp relay statistics**

```
user@host> show dhcp relay statistics

Messages received:
    BOOTREQUEST     0
    DHCPDECLINE     0
    DHCPDISCOVER    0
    DHCPINFORM      0
    DHCPRELEASE     0
    DHCPREQUEST     0

Messages sent:
    BOOTREPLY       0
    DHCPOFFER       0
    DHCPACK         0
    DHCPNACK        0
    DHCPFORCERENEW  0
```
show dhcp server binding

Syntax

```
show dhcp server binding
[interface <interface name>]
<brief | detail | summary | verbose>
<ip-address | MAC address>
<routing-instance routing-instance-name>
```

Release Information
Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.

Options
```
interface <interface name>—(Optional) Display information about active client bindings on the specified interface.

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcp server binding.

ip-address—Display DHCP binding information for a specific client identified by the specified IP address.

MAC address—Display DHCP binding information for a specific client identified by the specified MAC address.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.
```

Required Privilege Level
view

RELATED DOCUMENTATION
```
clear dhcp server binding | 2459
```

List of Sample Output
show dhcp server binding on page 2596
Output Fields

Table 70 on page 2596 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.

Table 70: show dhcp server binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the DHCP client.</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware address of the DHCP client.</td>
</tr>
<tr>
<td>Request received on</td>
<td>Interface on which the request was received.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of DHCP packet processing performed on the device.</td>
</tr>
<tr>
<td>Obtained at</td>
<td>Date and time at which the client’s IP address lease started.</td>
</tr>
<tr>
<td>Expires at</td>
<td>Date and time at which the client’s IP address lease expires.</td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the DHCP local server.</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp server binding

user@host> show dhcp server binding 100.20.32.1 detail

Active binding information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>100.20.32.1</td>
</tr>
<tr>
<td>Hardware address</td>
<td>90:00:00:01:00:01</td>
</tr>
<tr>
<td>Request received on</td>
<td>fe-0/0/2.0, relayed by 100.20.32.2</td>
</tr>
</tbody>
</table>

Lease information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>DHCP</td>
</tr>
<tr>
<td>Obtained at</td>
<td>2007-01-17 11:28:47 PST</td>
</tr>
<tr>
<td>Expires at</td>
<td>2007-01-17 11:38:47 PST</td>
</tr>
<tr>
<td>State</td>
<td>rebind</td>
</tr>
</tbody>
</table>
show dhcp server statistics

Syntax

```
show dhcp server statistics
<routing-instance>
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description

Display Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

- **routing-instance**—(Optional) Display information about DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level

- view

RELATED DOCUMENTATION

- clear dhcp server statistics  | 2460

List of Sample Output

**show dhcp server statistics on page 2598**

Output Fields

*Table 71 on page 2597* lists the output fields for the *show dhcp server statistics* command. Output fields are listed in the approximate order in which they appear.

**Table 71: show dhcp server statistics**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets dropped</td>
<td>Number of packets discarded by the DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
</tbody>
</table>
Table 71: show dhcp server statistics (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages received</td>
<td>Number of DHCP messages sent.</td>
</tr>
<tr>
<td></td>
<td>• BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received</td>
</tr>
<tr>
<td></td>
<td>• DHCPDECLINE—Number of DHCP PDUs of type DECLINE received</td>
</tr>
<tr>
<td></td>
<td>• DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received</td>
</tr>
<tr>
<td></td>
<td>• DHCPREQUEST—Number of DHCP PDUs of type REQUEST received</td>
</tr>
<tr>
<td></td>
<td>• DHCPINFORM—Number of DHCP PDUs of type INFORM received</td>
</tr>
<tr>
<td></td>
<td>• DHCPRELEASE—Number of DHCP PDUs of type RELEASE received</td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of DHCP messages received.</td>
</tr>
<tr>
<td></td>
<td>• BOOTREPLY—Number of BOOTP PDUs transmitted</td>
</tr>
<tr>
<td></td>
<td>• DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted</td>
</tr>
<tr>
<td></td>
<td>• DHCPACK—Number of DHCP PDUs of type ACK transmitted</td>
</tr>
<tr>
<td></td>
<td>• DHCPNACK—Number of DHCP PDUs of type NACK transmitted</td>
</tr>
<tr>
<td></td>
<td>• DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp server statistics

```
user@host> show dhcp server statistics

Packets dropped:
  Total                      0

Messages received:
  BOOTREQUEST                 0
  DHCPDECLINE                 0
  DHCPDISCOVER                0
  DHCPINFORM                  0
  DHCPRELEASE                 0
  DHCPREQUEST                 0

Messages sent:
  BOOTREPLY                   0
  DHCPOFFER                   0
  DHCPACK                     0
  DHCPNACK                    0
```

2598
<table>
<thead>
<tr>
<th>DHCPNAK</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPFORCERENEW</td>
<td>0</td>
</tr>
</tbody>
</table>
show dhcppv6 client binding

Syntax

show dhcppv6 client binding
  interface interface-name
  routing-instance <routing-instance-name>
  [brief | detail | summary]

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.

Options
interface interface-name—(Optional) Perform this operation on the specified interface.

routing-instance routing-instance-name—(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.

brief—(Optional) Display brief information about the active client bindings.

detail—(Optional) Display detailed client binding information.

summary—(Optional) Display a summary of DHCPv6 client information.

Required Privilege Level
view

RELATED DOCUMENTATION

clear dhcppv6 client binding | 2461

List of Sample Output
show dhcppv6 client binding on page 2601

Output Fields
Table 72 on page 2601 lists the output fields for the show dhcppv6 client binding command. Output fields are listed in the approximate order in which they appear.
Table 72: show dhcpv6 client binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Address</td>
<td>Hardware address of the DHCPv6 client.</td>
</tr>
<tr>
<td>State</td>
<td>State of the address-binding table on the DHCPv6 local server.</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client's IP address lease expires.</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds until the lease expires.</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client's IP address lease started.</td>
</tr>
<tr>
<td>Client DUID</td>
<td>The DHCPv6 client's unique identifier.</td>
</tr>
<tr>
<td>Bind type</td>
<td>The bind type.</td>
</tr>
<tr>
<td>Client Type</td>
<td>The type of DHCPv6 client. The client type can be autoconfig or stateful.</td>
</tr>
<tr>
<td>Rapid Commit</td>
<td>Two-message exchange option for address assignment.</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address of the DHCPv6 server.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>IP address of the DHCPv6 client.</td>
</tr>
</tbody>
</table>

Sample Output

```
show dhcpv6 client binding

user@host> show dhcpv6 client binding

IP prefix            Expires  ClientType  State  Interface       Client DUID
2001:db8::b2b7:8631:d968:8d5e/128  96   STATEFUL   BOUND ge-0/0/1.0
LL.TIME0x3-0x0-2c:6b:f5:62:39:cl

user@host> show dhcpv6 client binding detail
```

Client Interface: ge-0/0/1.0
Hardware Address: 2c:6b:f5:62:39:c1
State: BOUND (DHCPV6_CLIENT_STATE_BOUND)
Lease Expires: 2012-08-07 15:52:19 UTC
Lease Expires in: 116 seconds
Lease Start: 2012-08-07 15:50:19 UTC
Client DUID VENDOR0x00000583-0x3000103f
Bind Type: IA_NA
ClientType: STATEFUL
Rapid Commit Off
Server Ip Address: fe80::230:48ff:fe5d:5bf7
Client IP Address: 2001:db8::655b:3c80:2deb:1a3/128

DHCP options:
Name: server-identifier, Value: LL_TIME0x1-0x17acddab-00:30:48:5d:5b:f7
Name: vendor-opts, Value: 000005830002aaaa
Name: sip-server-list, Value: 2000::300 2000::302 2000::303 2000::304
Name: dns-recursive-server, Value: 2000::ff2000::fe
Name: domain-search-list, Value: 076578616d7066c6503636f6d00
show dhcpv6 client statistics

Syntax

```
show dhcpv6 client statistics
routing-instance <routing-instance-name>
```

Release Information
Statement introduced in Junos OS Release 12.1X45-D10 for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Description
Display Dynamic Host Configuration Protocol (DHCPv6) client statistics.

Options
```
routing-instance <routing-instance-name>
```
(Optional) Display the statistics for DHCPv6 clients on the specified routing instance.

Required Privilege Level
```
view
```

Related Documentation
```
clear dhcpv6 client statistics
```

List of Sample Output
```
show dhcpv6 client statistics on page 2604
```

Output Fields
```
Table 73 on page 2603 lists the output fields for the `show dhcpv6 client statistics` command. Output fields are listed in the approximate order in which they appear.

Table 73: show dhcpv6 client statistics Output Fields
```
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dhcpv6 Packets dropped</td>
<td>Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the DHCPv6 Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
</tbody>
</table>
```
Table 73: show dhcpv6 client statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCPv6 messages sent.</td>
</tr>
<tr>
<td>DHCPV6_DECLINE</td>
<td>Number of DHCPv6 PDUs of type DECLINE transmitted</td>
</tr>
<tr>
<td>DHCPV6_SOLICIT</td>
<td>Number of DHCPv6 PDUs of type SOLICIT transmitted</td>
</tr>
<tr>
<td>DHCPV6_INFORMATION_REQUEST</td>
<td>Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted</td>
</tr>
<tr>
<td>DHCPV6_RELEASE</td>
<td>Number of DHCPv6 PDUs of type RELEASE transmitted</td>
</tr>
<tr>
<td>DHCPV6_REQUEST</td>
<td>Number of DHCPv6 PDUs of type REQUEST transmitted</td>
</tr>
<tr>
<td>DHCPV6_CONFIRM</td>
<td>Number of DHCPv6 PDUs of type CONFIRM transmitted</td>
</tr>
<tr>
<td>DHCPV6_RENEW</td>
<td>Number of DHCPv6 PDUs of type RENEW transmitted</td>
</tr>
<tr>
<td>DHCPV6_REBIND</td>
<td>Number of DHCPv6 PDUs of type REBIND transmitted</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td>DHCPV6_ADVERTISE</td>
<td>Number of DHCPv6 PDUs of type ADVERTISE received</td>
</tr>
<tr>
<td>DHCPV6_REPLY</td>
<td>Number of DHCPv6 PDUs of type REPLY received</td>
</tr>
<tr>
<td>DHCPV6_RECONFIGURE</td>
<td>Number of DHCPv6 PDUs of type RECONFIGURE received</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show dhcpv6 client statistics
user@host> show dhcpv6 client statistics

Dhcpv6 Packets dropped:
  Total               0
```
Messages sent:
- DHCPv6_DECLINE 0
- DHCPv6_SOLICIT 3
- DHCPv6_INFORMATION_REQUEST 6
- DHCPv6_RELEASE 1
- DHCPv6_REQUEST 2
- DHCPv6_CONFIRM 0
- DHCPv6_RENEW 0
- DHCPv6_REBIND 0

Messages received:
- DHCPv6_ADVERTISE 3
- DHCPv6_REPLY 3
- DHCPv6_RECONFIGURE 0
show dhcpv6 relay binding

Syntax

show dhcpv6 relay binding
<address>
<brief>
<detail>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<summary>

Release Information
Command introduced in Junos OS Release 11.4.
interfaces-vlan and interfaces-wildcard options introduced in Junos OS Release 12.1.

Description
Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options
address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:

- CID—The specified Client ID (CID).
- ipv6-prefix—The specified IPv6 prefix.
- session-id—The specified session ID.

brief—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as show dhcpv6 relay binding.

detail—(Optional) Display detailed client binding information.

interface interface-name—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and S-VLAN ID.

interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.

interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).
logical-system logical-system-name—(Optional) Perform this operation on the specified logical system.

routing-instance routing-instance-name—(Optional) Perform this operation on the specified routing instance.

summary—(Optional) Display a summary of DHCPv6 client information.

**Required Privilege Level**

view

**RELATED DOCUMENTATION**

Viewing and Clearing DHCP Bindings

clear dhcpv6 relay binding | 2463

**List of Sample Output**

show dhcpv6 relay binding on page 2610
show dhcpv6 relay binding (Address) on page 2610
show dhcpv6 relay binding detail (Client ID) on page 2611
show dhcpv6 relay binding detail on page 2611
show dhcpv6 relay binding detail (Dual-Stack) on page 2612
show dhcpv6 relay binding detail (Multi-Relay Topology) on page 2612
show dhcpv6 relay binding (Session ID) on page 2613
show dhcpv6 relay binding (Subscriber with Multiple Addresses) on page 2613
show dhcpv6 relay binding detail (Subscriber with Multiple Addresses) on page 2614
show dhcpv6 relay binding (Interfaces VLAN) on page 2615
show dhcpv6 relay binding (Interfaces Wildcard) on page 2615
show dhcpv6 relay binding (Interfaces Wildcard) on page 2616
show dhcpv6 relay binding summary on page 2616

**Output Fields**

Table 74 on page 2607 lists the output fields for the `show dhcpv6 relay binding` command. Output fields are listed in the approximate order in which they appear.

**Table 74: show dhcpv6 relay binding Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number clients,(number init, number bound, number selecting, number requesting, number renewing, number rebinding)</strong></td>
<td>Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>Client IPv6 Prefix</td>
<td>Prefix of the DHCPv6 client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
<td>Level of Output</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Client IPv6 Excluded Prefix</td>
<td>IPv6 Prefix of the DHCP client excluded.</td>
<td>detail</td>
</tr>
<tr>
<td>Client DUID</td>
<td>DHCP for IPv6 Unique Identifier (DUID) of the client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Client IPv6 Address</td>
<td>IPv6 address assigned to the subscriber.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber session.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which the lease expires.</td>
<td>brief detail</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv6 relay address binding table on the DHCPv6 client:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>• BOUND—Client has an active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• INIT—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REBINDING—Client is broadcasting a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RECONFIGURE—Client is broadcasting a request to reconfigure the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RELEASE—Client is releasing the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RENEWING—Client is sending a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REQUESTING—Client is requesting a DHCPv6 server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SELECTING—Client is receiving offers from DHCPv6 servers.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Incoming client interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client's IP address lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds in which the lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires</td>
<td>Date and UTC time at which the client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires in</td>
<td>Number of seconds at which the client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client’s IP address lease started.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 74: show dhcpv6 relay binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lease time violated</strong></td>
<td>Lease time violation has occurred.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Incoming Client Interface</strong></td>
<td>Client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server Address</strong></td>
<td>IP address of the DHCPv6 server. Displays <em>unknown</em> for a DHCPv6 relay agent in a multi-relay topology that is not directly adjacent to the DHCPv6 server and does not detect the IP address of the server. In that case, the output instead displays the <strong>Next Hop Server Facing Relay</strong> field.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Next Hop Server Facing Relay</strong></td>
<td>Next-hop address in the direction of the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server Interface</strong></td>
<td>Interface of the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Relay Address</strong></td>
<td>IP address of the relay.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client Pool Name</strong></td>
<td>Address pool that granted the client lease.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client ID Length</strong></td>
<td>Length of client ID.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Client Id</strong></td>
<td>Client ID.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Generated Circuit ID</strong></td>
<td>Circuit ID generated by the DHCPv6 Interface-ID option (option 18)</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Generated Remote ID Enterprise Number</strong></td>
<td>The Juniper Networks IANA private enterprise number</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Generated Remote ID</strong></td>
<td>Remote ID generated by the DHCPv6 Remote-ID option (option 37)</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Dual Stack Group</strong></td>
<td>Name of the dual-stack group for the DHCPv6 binding.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Dual Stack Peer Address</strong></td>
<td>Address of the dual-stack DHCPv4 peer.</td>
<td>detail</td>
</tr>
</tbody>
</table>
show dhcpv6 relay binding

user@host> show dhcpv6 relay binding

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:3c4d:15::/64</td>
<td>1</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:3c4d:16::/64</td>
<td>2</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:3c4d:17::/64</td>
<td>3</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03</td>
</tr>
<tr>
<td>2001:db8:3c4d:18::/64</td>
<td>4</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04</td>
</tr>
<tr>
<td>2001:db8:3c4d:19::/64</td>
<td>5</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05</td>
</tr>
<tr>
<td>2001:db8:3c4d:20::/64</td>
<td>6</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td></td>
</tr>
<tr>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06</td>
</tr>
</tbody>
</table>

show dhcpv6 relay binding (Address)

user@host> show dhcpv6 relay binding 2001:db8:1111:2222::/64 detail

<table>
<thead>
<tr>
<th>Session Id:</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client IPv6 Prefix:</td>
<td>2001:db8:3c4d:15::/64</td>
</tr>
<tr>
<td>Client DUID:</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
</tr>
<tr>
<td>State:</td>
<td>BOUND (RELAY_STATE_BOUND)</td>
</tr>
<tr>
<td>Lease Expires:</td>
<td>2011-05-25 07:12:09 PDT</td>
</tr>
<tr>
<td>Lease Expires in:</td>
<td>77115 seconds</td>
</tr>
<tr>
<td>Preferred Lease Expires:</td>
<td>2012-07-24 00:18:14 UTC</td>
</tr>
<tr>
<td>Preferred Lease Expires in:</td>
<td>600 seconds</td>
</tr>
<tr>
<td>Lease Start:</td>
<td>2011-05-24 07:12:09 PDT</td>
</tr>
<tr>
<td>Incoming Client Interface:</td>
<td>ge-1/0/0.0</td>
</tr>
<tr>
<td>Server Address:</td>
<td>2001:db8:aaaa:bbbb::1</td>
</tr>
<tr>
<td>Server Interface:</td>
<td>none</td>
</tr>
<tr>
<td>Relay Address:</td>
<td>2001:db8:1111:2222::</td>
</tr>
<tr>
<td>Client Pool Name:</td>
<td>pool-25</td>
</tr>
<tr>
<td>Client Id Length:</td>
<td>14</td>
</tr>
<tr>
<td>Client Id:</td>
<td>/0x00010001/0x4bfa26af/0x00109400/0x0001</td>
</tr>
</tbody>
</table>
show dhcpv6 relay binding detail (Client ID)

user@host> show dhcpv6 relay binding 14/0x00010001/0x4bfa26af/0x00109400/0x0001 detail

Session Id:  1
Client IPv6 Prefix:                    2001:db8:3c4d:15::/64
Client DUID:                           LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
State:                                 BOUND (RELAY_STATE_BOUND)
Lease Expires:                         2011-05-25 07:12:09 PDT
Lease Expires in:                      77115 seconds
Preferred Lease Expires:               2012-07-24 00:18:14 UTC
Preferred Lease Expires in:            600 seconds
Lease Start:                           2011-05-24 07:12:09 PDT
Lease time violated:                   yes
Incoming Client Interface:             ge-1/0/0.0
Server Address:                        2001:db8:aaaa:bbbb::1
Server Interface:                      none
Relay Address:                         2001:db8:1111:2222::
Client Pool Name:                      pool-25
Client Id Length:                      14
Client Id:                             /0x00010001/0x4bfa26af/0x00109400/0x0001

show dhcpv6 relay binding detail

user@host> show dhcpv6 relay binding detail

Session Id:  1
Client IPv6 Prefix:                    2001:db8:3c4d:15::/64
Client DUID:                           LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
State:                                 BOUND (RELAY_STATE_BOUND)
Lease Expires:                         2011-05-25 07:12:09 PDT
Lease Expires in:                      77115 seconds
Preferred Lease Expires:               2012-07-24 00:18:14 UTC
Preferred Lease Expires in:            600 seconds
Lease Start:                           2011-05-24 07:12:09 PDT
Lease time violated:                   yes
Incoming Client Interface:             ge-1/0/0.0
Server Address:                        2001:db8:aaaa:bbbb::1
Server Interface:                      none
Relay Address:                         2001:db8:1111:2222::
Client Pool Name:                      pool-25
Client Id Length:                      14
Client Id:                             /0x00010001/0x4bfa26af/0x00109400/0x0001
show dhcpv6 relay binding detail (Dual-Stack)

user@host> show dhcpv6 relay binding detail

Session Id: 2
Client IPv6 Prefix: 2001:db8:ffff:0::/64
Client IPv6 Address: 2001:db8::3000::1/128
Client DUID: LL0x1-00:00:64:01:01:02
State: BOUND (DHCPV6_RELAY_STATE_BOUND)
Lease Expires: 2016-10-17 07:39:25 PDT
Lease Expires in: 3450 seconds
Lease Start: 2016-10-17 06:39:25 PDT
Last Packet Received: 2016-10-17 06:39:25 PDT
Incoming Client Interface: ae0.3221225472
Client Interface Svlan Id: 2000
Client Interface Vlan Id: 1
Server Ip Address: 2001:db8:3000::2
Server Interface: none
Client Profile Name: my-dual-stack
Client Id Length: 10
Client Id: /0x00030001/0x00006401/0x0102
Dual Stack Group: group1
Dual Stack Peer Address: 192.0.2.4

show dhcpv6 relay binding detail (Multi-Relay Topology)

user@host > show dhcpv6 relay binding detail

Session Id: 13
Client IPv6 Prefix: 2001:db8:3000::8001::5/128
Client DUID: LL0x1-00:00:64:03:01:02
State: BOUND (DHCPV6_RELAY_STATE_BOUND)
Lease Expires: 2011-11-21 06:14:50 PST
Lease Expires in: 293 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2011-11-21 06:09:50 PST
Incoming Client Interface: ge-1/0/0.0
Server Address: unknown
Next Hop Server Facing Relay: 2001:db8:4000::2
Server Interface: none
Client Id Length: 10
Client Id: /0x00030001/0x00006503/0x0102

show dhcpv6 relay binding (Session ID)

user@host> show dhcpv6 relay binding 41

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:3c4d:15::/64</td>
<td>41</td>
<td>78837</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>

show dhcpv6 relay binding (Subscriber with Multiple Addresses)

user@host> show dhcpv6 relay binding

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8:1001::1:24/128</td>
<td>23</td>
<td>593</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:1001::1:1c/128</td>
<td>23</td>
<td>393</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:1001::1:14/128</td>
<td>23</td>
<td>193</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:3001::300/120</td>
<td>23</td>
<td>293</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:3001::200/120</td>
<td>23</td>
<td>193</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:db8:3001::100/120</td>
<td>23</td>
<td>93</td>
<td>BOUND</td>
<td>ge-9/0/9.0</td>
<td>LL_TIME0x1-0x55306754-00:10:94:00:00:02</td>
</tr>
</tbody>
</table>

When DHCPv6 relay binding is configured with prefix exclude option, we get the following output:

user@host> show dhcpv6 relay binding detail

Session Id: 6
Hardware Address: 00:10:94:00:00:01
Client IPv6 Address: 7001:2:3::d/128
Lease Expires: 2017-12-11 07:45:27 IST
Lease Expires in: 9999952 seconds
Preferred Lease Expires: 2017-12-11 07:45:27 IST
Preferred Lease Expires in: 9999952 seconds
Client IPv6 Prefix: 7001::1000:0:0:0/68
Client IPv6 Excluded Prefix: 7001::fff:ffff:ffff:ff00/120
Lease Expires: 2017-12-11 07:45:27 IST
Lease Expires in: 9999952 seconds
Preferred Lease Expires: 2017-12-11 07:45:27 IST
Preferred Lease Expires in: 9999952 seconds
Client DUID: LL_TIME0x1-0x599553b0-00:10:94:00:00:01
State: BOUND (DHCPV6_RELAY_STATE_BOUND)
Lease Start: 2017-08-17 13:58:33 IST
Last Packet Received: 2017-08-17 13:58:48 IST
Incoming Client Interface: ge-0/0/0.100
Client Interface Vlan Id: 100
Server Ip Address: 7002::1
Server Interface: none
Client Id Length: 14
Client Id: /0x00010001/0x599553b0/0x00109400/0x0001
Generated Circuit ID: ge-0/0/0:100

show dhcpv6 relay binding detail (Subscriber with Multiple Addresses)

user@host> show dhcpv6 relay binding detail

<table>
<thead>
<tr>
<th>Session Id</th>
<th>Client IPv6 Address</th>
<th>Lease Expires</th>
<th>Lease Expires in</th>
<th>Preferred Lease Expires</th>
<th>Preferred Lease Expires in</th>
</tr>
</thead>
</table>
show dhcpv6 relay binding (Interfaces VLAN)

user@host> show dhcpv6 relay binding ge-1/0/0:100-200

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8::/32</td>
<td>11</td>
<td>87583</td>
<td>BOUND</td>
<td>ge-1/0/0.1073741827</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:DB8:19::/32</td>
<td>12</td>
<td>87583</td>
<td>BOUND</td>
<td>ge-1/0/0.1073741827</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>

show dhcpv6 relay binding (Interfaces Wildcard)

user@host> show dhcpv6 relay binding demux0
### show dhcpv6 relay binding (Interfaces Wildcard)

```
user@host> show dhcpv6 relay binding ge-1/3/*
```

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:DB8::/32</td>
<td>22</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:DB8:19::/32</td>
<td>33</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:DB8:C9::/32</td>
<td>34</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>

### show dhcpv6 relay binding summary

```
user@host> show dhcpv6 relay binding summary
```

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
show dhcpv6 relay statistics

Syntax

```
show dhcpv6 relay statistics
  <bulk-leasequery-connections>
  <leasequery>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information
Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Options
`bulk-leasequery-connections`—(Optional) Display DHCPv6 relay bulk leasequery statistics.
`leasequery`—(Optional) Display information about DHCPv6 relay individual leasequery statistics.
`logical-system logical-system-name`—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.
`routing-instance routing-instance-name`—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.

Required Privilege Level
view

RELATED DOCUMENTATION
- `clear dhcpv6 relay statistics` | 2467
- `DHCPv6 Client MAC Address Validation to Prevent Session Hijacking`

List of Sample Output
- `show dhcpv6 relay statistics on page 2620`
- `show dhcpv6 relay statistics bulk-leasequery-connections on page 2620`

Output Fields
Table 75 on page 2618 lists the output fields for the `show dhcpv6 relay statistics` command. Output fields are listed in the approximate order in which they appear.

Table 75: show dhcpv6 relay statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCPv6 Packets dropped</strong></td>
<td>Number of packets discarded by the extended DHCPv6 relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total</strong>—Total number of packets discarded by the DHCPv6 relay agent application.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad options</strong>—Number of packets discarded because invalid options were specified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad send</strong>—Number of packets that the extended DHCP relay application could not send.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad src address</strong>—Number of packets discarded because the family type was not AF_INET6.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client MAC validation</strong>—Number of packets discarded because validation of the client MAC address failed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No client id</strong>—Number of packets discarded because they could not be matched to a client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Lease Time Violation</strong>—Number of packets discarded because of a lease time violation</td>
</tr>
<tr>
<td></td>
<td>• <strong>No safd</strong>—Number of packets discarded because they arrived on an unconfigured interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Short packet</strong>—Number of packets discarded because they were too short.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Relay hop count</strong>—Number of packets discarded because the hop count in the packet exceeded 32.</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_DECLINE</strong>—Number of DHCPv6 PDUs of type DECLINE received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_SOLICIT</strong>—Number of DHCPv6 PDUs of type SOLICIT received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_INFORMATION_REQUEST</strong>—Number of DHCPv6 PDUs of type INFORMATION-REQUEST received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_RELEASE</strong>—Number of DHCPv6 PDUs of type RELEASE received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_REQUEST</strong>—Number of DHCPv6 PDUs of type REQUEST received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_CONFIRM</strong>—Number of DHCPv6 PDUs of type CONFIRM received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_RENEW</strong>—Number of DHCPv6 PDUs of type RENEW received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_REBIND</strong>—Number of DHCPv6 PDUs of type REBIND received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_RELAY_REPL</strong>—Number of DHCPv6 PDUs of type RELAY-REPL received</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6_RELAY_FORW</strong>—Number of DHCPv6 RELAY-FORW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6LEASEQUERY_REPL</strong>—Number of DHCPv6 replies received from the DHCPv6 sever</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6LEASEQUERY_DATA</strong>—xxxxxx</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPv6LEASEQUERY_DONE</strong>—The leasequery is complete</td>
</tr>
</tbody>
</table>
### Table 75: show dhcv6 relay statistics Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCPv6 messages sent.</td>
</tr>
<tr>
<td>• <strong>DHCPv6_ADVERTISE</strong></td>
<td>Number of DHCPv6 ADVERTISE PDUs transmitted</td>
</tr>
<tr>
<td>• <strong>DHCP_REPLY</strong></td>
<td>Number of DHCPv6 REPLY PDUs transmitted</td>
</tr>
<tr>
<td>• <strong>DHCP_RECONFIGURE</strong></td>
<td>Number of DHCPv6 RECONFIGURE PDUs transmitted</td>
</tr>
<tr>
<td>• <strong>DHCP_RELAY_FORW</strong></td>
<td>Number of DHCPv6 RELAY-FORW PDUs transmitted</td>
</tr>
<tr>
<td>• <strong>DHCPv6_RELAY_REPL</strong></td>
<td>Number of DHCPv6 RELAY-REPL PDUs transmitted</td>
</tr>
<tr>
<td>• <strong>DHCPv6LEASEQUERY</strong></td>
<td>Number of DHCP leasequery messages transmitted</td>
</tr>
<tr>
<td><strong>Packets forwarded</strong></td>
<td>Number of packets forwarded by the extended DHCPv6 relay agent application.</td>
</tr>
<tr>
<td>• <strong>FWD_REQUEST</strong></td>
<td>Number of DHCPv6 REQUEST packets forwarded</td>
</tr>
<tr>
<td>• <strong>FWD_REPLY</strong></td>
<td>Number of DHCPv6 REPLY packets forwarded</td>
</tr>
<tr>
<td><strong>External Server Response</strong></td>
<td>State of the external DHCP server responsiveness.</td>
</tr>
<tr>
<td><strong>Total Requested Servers</strong></td>
<td>Total number of servers with which the DHCP relay agent has requested a bulk leasequery connection.</td>
</tr>
<tr>
<td><strong>Total Attempted Servers</strong></td>
<td>Total number of servers with which the DHCP relay agent has attempted to create a bulk leasequery connection.</td>
</tr>
<tr>
<td><strong>Total Connected</strong></td>
<td>Total number of servers that have formed a bulk leasequery connection with the DHCP relay agent.</td>
</tr>
<tr>
<td><strong>Total Terminated by Server</strong></td>
<td>Total number of servers that have terminated a bulk leasequery connection with the DHCP relay agent.</td>
</tr>
<tr>
<td><strong>Total Max Attempted</strong></td>
<td>Total number of servers where the DHCP relay agent reached the maximum retry limit when it attempted to create a bulk leasequery connection.</td>
</tr>
<tr>
<td><strong>Total Closed due to Errors</strong></td>
<td>Total number of bulk leasequery connections that closed due to an internal error on the DHCP relay agent.</td>
</tr>
<tr>
<td><strong>In-Flight Connected</strong></td>
<td>Number of current bulk leasequery connections on the DHCP relay agent.</td>
</tr>
<tr>
<td><strong>Bulk Leasequery Reply Packet Retries</strong></td>
<td>Number of bulk leasequery reply packets that the DHCP relay agent has retried.</td>
</tr>
</tbody>
</table>
Sample Output

show dhcpv6 relay statistics

user@host> show dhcpv6 relay statistics

DHCPv6 Packets dropped:
  Total 2
  Lease Time Violation 1
  Client MAC validation 1

Messages received:
  DHCPV6_DECLINE 0
  DHCPV6_SOLICIT 10
  DHCPV6_INFORMATION_REQUEST 0
  DHCPV6_RELEASE 0
  DHCPV6_REQUEST 10
  DHCPV6_CONFIRM 0
  DHCPV6_RENEW 0
  DHCPV6_REBIND 0
  DHCPV6_RELAY_FORW 0
  DHCPV6_LEASEQUERY_REPLY 0
  DHCPV6_LEASEQUERY_DATA 0
  DHCPV6_LEASEQUERY_DONE 0

Messages sent:
  DHCPV6_ADVERTISE 0
  DHCPV6_REPLY 0
  DHCPV6_RECONFIGURE 0
  DHCPV6_RELAY_REPL 0
  DHCPV6_LEASEQUERY 0

Packets forwarded:
  Total 4
  FWD REQUEST 2
  FWD REPLY 2

External Server Response:
  State Responding

show dhcpv6 relay statistics bulk-leasequery-connections

user@host> show dhcpv6 relay statistics bulk-leasequery-connections
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Requested Servers</td>
<td>0</td>
</tr>
<tr>
<td>Total Attempted Servers</td>
<td>0</td>
</tr>
<tr>
<td>Total Connected</td>
<td>0</td>
</tr>
<tr>
<td>Total Terminated by Server</td>
<td>0</td>
</tr>
<tr>
<td>Total Max Attempted</td>
<td>0</td>
</tr>
<tr>
<td>Total Closed due to Errors</td>
<td>0</td>
</tr>
<tr>
<td>In-Flight Connected</td>
<td>0</td>
</tr>
<tr>
<td>Bulk Leasequery Reply Packet Retries</td>
<td>0</td>
</tr>
</tbody>
</table>
show dhcpv6 server binding

Syntax

```
show dhcpv6 server binding
<address>
<brief | detail | summary>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.

Description

Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server.

Options

`address`—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:

- `CID`—The specified Client ID (CID).
- `ipv6-prefix`—The specified IPv6 prefix.
- `session-id`—The specified session ID.

`brief | detail | summary`—(Optional) Display the specified level of output about active client bindings. The default is `brief`, which produces the same output as `show dhcpv6 server binding`.

`interface interface-name`—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

`interfaces-vlan`—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.

`interfaces-wildcard`—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (`*`).

`logical-system logical-system-name`—(Optional) Display information about active client bindings for DHCPv6 clients on the specified logical system.
routin-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

**Required Privilege Level**

view

**RELATED DOCUMENTATION**

Viewing and Clearing DHCP Bindings

| clear dhcpv6 server binding | 2470 |

**List of Sample Output**

show dhcpv6 server binding on page 2625
show dhcpv6 server binding detail on page 2626
show dhcpv6 server binding interface on page 2627
show dhcpv6 server binding interface detail on page 2627
show dhcpv6 server binding (IPv6 Prefix) on page 2628
show dhcpv6 server binding (Session ID) on page 2628
show dhcpv6 server binding (Interfaces VLAN) on page 2629
show dhcpv6 server binding (Interfaces Wildcard) on page 2629
show dhcpv6 server binding summary on page 2629

**Output Fields**

Table 76 on page 2623 lists the output fields for the `show dhcpv6 server binding` command. Output fields are listed in the approximate order in which they appear.

**Table 76: show dhcpv6 server binding Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>number</em> clients, <em>(number init, number bound, number selecting, number requesting, number renewing, number releasing)</em></td>
<td>Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>Prefix</td>
<td>Client’s DHCPv6 prefix, or prefix used to support multiple address assignment.</td>
<td>brief detail</td>
</tr>
</tbody>
</table>
Table 76: show dhcpv6 server binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber session.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which lease expires.</td>
<td>brief detail</td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the extended DHCPv6 local server:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>• BOUND—Client has active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• INIT—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RECONFIGURE—Server has sent reconfigure message to client.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RELEASE—Client is releasing IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RENEWING—Client sending request to renew IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REQUESTING—Client requesting a DHCPv6 server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SELECTING—Client receiving offers from DHCPv6 servers.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the DHCPv6 request was received.</td>
<td>brief</td>
</tr>
<tr>
<td>Client IPv6 Address</td>
<td>Client's IPv6 address.</td>
<td>detail</td>
</tr>
<tr>
<td>Client IPv6 Prefix</td>
<td>Client's IPv6 prefix.</td>
<td>detail</td>
</tr>
<tr>
<td>Client IPv6 Excluded Prefix</td>
<td>IPv6 Prefix of the DHCP client excluded.</td>
<td>detail</td>
</tr>
<tr>
<td>Client DUID</td>
<td>Client’s DHCP Unique Identifier (DUID).</td>
<td>brief detail</td>
</tr>
<tr>
<td>Lease expires</td>
<td>Date and time at which the client’s IP address lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease expires in</td>
<td>Number of seconds in which lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires</td>
<td>Date and UTC time at which the client’s IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires in</td>
<td>Number of seconds at which client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client's address lease was obtained.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease time violated</td>
<td>Lease time violation has occurred.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 76: show dhcpv6 server binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Client Interface</td>
<td>Client’s incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Interface</td>
<td>Interface of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Pool Name</td>
<td>Address pool used to assign IPv6 address.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Prefix Pool Name</td>
<td>Address pool used to assign IPv6 prefix.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Id length</td>
<td>Length of the DHCPv6 client ID, in bytes.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Id</td>
<td>ID of the DHCPv6 client.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Id</td>
<td>DHCP unique identifier (DUID) for the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Interface Svlan Id</td>
<td>S-VLAN ID of the client’s incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Interface Vlan Id</td>
<td>VLAN ID of the client’s incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Dual Stack Group</td>
<td>DHCPv6 server profile name.</td>
<td>detail</td>
</tr>
<tr>
<td>Dual Stack Peer Address</td>
<td>DHCPv6 Peer IP address.</td>
<td>detail</td>
</tr>
</tbody>
</table>

**Sample Output**

`show dhcpv6 server binding`

```
user@host> show dhcpv6 server binding

Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
2001:db8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0

```

LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
<table>
<thead>
<tr>
<th>Client IPv6 Prefix</th>
<th>Client IPv6 Address</th>
<th>Client DUID</th>
<th>State</th>
<th>Lease Expires</th>
<th>Lease Expires in:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::fff0:4:00:00:00:02</td>
<td>2001:db8:0:8003::1/128</td>
<td>LL0x1-00:00:64:01:01:02</td>
<td>BOUND (DHCPV6_LOCAL_SERVER_STATE_BOUND)</td>
<td>2016-11-07 08:30:39 PST</td>
<td>43706 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When DHCPv6 binding is configured with prefix exclude option, we get the following output:
### Session Id:  5
Client IPv6 Address:  2001:db8:2:3::d/128
 Lease Expires:  2017-12-11 07:45:15 IST
 Lease Expires in:  9999995 seconds
 Preferred Lease Expires:  2017-12-11 07:45:15 IST
 Preferred Lease Expires in:  9999995 seconds
 Client IPv6 Prefix:  2001:db8::1000:0:0/68
 Client IPv6 Excluded Prefix:  2001:db8::1fff:ffff:ff00/120
 Lease Expires:  2017-12-11 07:45:15 IST
 Lease Expires in:  9999995 seconds
 Preferred Lease Expires:  2017-12-11 07:45:15 IST
 Preferred Lease Expires in:  9999995 seconds
 Client DUID:  LL_TIME0x1-0x599553b0-00:10:94:00:00:01
 State:  BOUND (DHCPV6_LOCAL_SERVER_STATE_BOUND)
 Lease Start:  2017-08-17 13:58:32 IST
 Last Packet Received:  2017-08-17 13:58:36 IST
 Incoming Client Interface:  ge-0/0/0.0
 Client Interface Vlan Id:  100
 Client Pool Name:  ia_na_pool
 Client Prefix Pool Name:  prefix_delegate_pool
 Client Id Length:  14
 Client Id:  /0x00010001/0x599553b0/0x00109400/0x0001
 Relay Id Length:  31
 Relay Id:
 /0x00020000/0x05830130/0x303a3035/0x3a38363a
 /0x34343a65/0x323a6330/0x00000000/0x000000

### show dhcpv6 server binding interface
```bash
user@host> show dhcpv6 server binding interface
dhcpv6 server binding interface
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:1111:2222::/64 1           86055    BOUND    ge-0/0/0.100
LL_TIME0x1-0x599553b0-00:10:94:00:00:01
```

### show dhcpv6 server binding interface detail
```bash
user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
dhcpv6 server binding interface
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:1111:2222::/64 1           86055    BOUND    ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01
```
Session Id:  7
Client IPv6 Prefix: 2001:db8:1111:2222::/64
Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
State: BOUND (bound)
Lease Expires: 2009-07-21 10:41:15 PDT
Lease Expires in: 86136 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 0.0.0.0
Server Interface: none
Client Id Length: 14
Client Id: /0x00010001/0x02e159c0/0x00109400/0x0002

show dhcpv6 server binding (IPv6 Prefix)

user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005 detail

Session Id:  7
Client IPv6 Prefix: 2001:db8:1111:2222::/64
Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
State: BOUND (bound)
Lease Expires: 2009-07-21 10:41:15 PDT
Lease Expires in: 86136 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 0.0.0.0
Server Interface: none
Client Id Length: 14
Client Id: /0x00010001/0x02e159c0/0x00109400/0x0003

show dhcpv6 server binding (Session ID)

user@host> show dhcpv6 server binding 8

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::/32</td>
<td>8</td>
<td>86235</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x2e159c0-00:10:94:00:00:03</td>
</tr>
</tbody>
</table>
show dhcpv6 server binding (Interfaces VLAN)

```
user@host> show dhcpv6 server binding ge-1/0/0:100-200

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::/32</td>
<td>11</td>
<td>87583</td>
<td>BOUND</td>
<td>ge-1/0/0.1073741827</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:19::/32</td>
<td>12</td>
<td>87583</td>
<td>BOUND</td>
<td>ge-1/0/0.1073741827</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding demux0

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::/32</td>
<td>30</td>
<td>79681</td>
<td>BOUND</td>
<td>demux0.1073741824</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:19::/32</td>
<td>31</td>
<td>79681</td>
<td>BOUND</td>
<td>demux0.1073741825</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:C9::/32</td>
<td>32</td>
<td>79681</td>
<td>BOUND</td>
<td>demux0.1073741826</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding ge-1/3/*

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:db8::/32</td>
<td>22</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:19::/32</td>
<td>33</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:db8:C9::/32</td>
<td>24</td>
<td>79681</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
<td>LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```
show dhcpv6 server binding (View)

Syntax

```
show dhcpv6 server binding
   <brief | detail | summary>
   <interface interface-name>
   <routing-instance routing-instance-name>
```

Release Information
Command introduced in Junos OS Release 10.4.

Description
Display the address bindings in the client table for DHCPv6 local server.

Options

- brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as `show dhcpv6 server binding`.

- interface interface-name—(Optional) Display information about active client bindings on the specified interface.

- routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege Level
view

RELATED DOCUMENTATION

- clear dhcpv6 server binding (Local Server) | 2473

List of Sample Output

- show dhcpv6 server binding on page 2632
- show dhcpv6 server binding detail on page 2632
- show dhcpv6 server binding interface on page 2633
- show dhcpv6 server binding interface detail on page 2633
- show dhcpv6 server binding prefix on page 2634
- show dhcpv6 server binding session-id on page 2634
- show dhcpv6 server binding summary on page 2635

Output Fields
**Table 76 on page 2623** lists the output fields for the `show dhcpv6 server binding` command. Output fields are listed in the approximate order in which they appear.

**Table 77: show dhcv6p server binding Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| **number clients**,  
  *(number init,  
  number bound,  
  number selecting,  
  number requesting,  
  number renewing,  
  number releasing)* | Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state. | **summary** |
| Prefix | Client’s DHCPv6 prefix. | **brief**  
  **detail** |
| Session Id | Session ID of the subscriber session. | **brief**  
  **detail** |
| Expires | Number of seconds in which lease expires. | **brief**  
  **detail** |
| State | State of the address binding table on the DHCPv6 local server:  
  • **BOUND**—Client has active IP address lease.  
  • **INIT**—Initial state.  
  • **RELEASE**—Client is releasing IP address lease.  
  • **RECONFIGURE**—Client has received reconfigure message from server.  
  • **RENEWING**—Client sending request to renew IP address lease.  
  • **REQUESTING**—Client requesting a DHCPv6 server.  
  • **SELECTING**—Client receiving offers from DHCPv6 servers. | **brief**  
  **detail** |
| Interface | Interface on which the DHCPv6 request was received. | **brief** |
| Client DUID | Client’s DHCP Unique Identifier (DUID). | **brief** |
| Lease expires | Date and time at which the client’s IP address lease expires. | **detail** |
| Lease expires in | Number of seconds in which lease expires. | **detail** |
| Lease Start | Date and time at which the client’s address lease was obtained. | **detail** |
Table 77: show dhcv6p server binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Client Interface</strong></td>
<td>Client’s incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server IP Address</strong></td>
<td>IP address of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server Interface</strong></td>
<td>Interface of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>ClientId length</strong></td>
<td>Length of the DHCPv6 client ID, in bytes.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>ClientId</strong></td>
<td>ID of the DHCPv6 client.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>ServerId</strong></td>
<td>ID type and ID of the DHCPv6 server.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

**show dhcv6 server binding**

```
user@host> show dhcv6 server binding
```

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64  6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64  7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64  8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64  9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

```
show dhcv6 server binding detail
user@host> show dhcv6 server binding detail
```

```
show dhcpv6 server binding interface

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
data

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:bd8:1111:2222::/64</td>
<td>1</td>
<td>86055</td>
<td>BOUND</td>
<td>ge-1/0/0.100</td>
<td>LL_TIME0x1-0x2e159c0-00:10:94:00:00:01</td>
</tr>
</tbody>
</table>

show dhcpv6 server binding interface detail

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail

show dhcpv6 server binding prefix

user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005 detail

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:bd8:1111:2222::/64</td>
<td>8</td>
<td>86235</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x2e159c0-00:10:94:00:00:02</td>
</tr>
</tbody>
</table>

show dhcpv6 server binding session-id

user@host> show dhcpv6 server binding 8

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:bd8:1111:2222::/64</td>
<td>8</td>
<td>86235</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x2e159c0-00:10:94:00:00:02</td>
</tr>
</tbody>
</table>
show dhcpv6 server binding summary

user@host> show dhcpv6 server binding summary

5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
show dhcpv6 server statistics

Syntax

```
show dhcpv6 server statistics
 <bulk-leasequery-connections>
 <logical-system logical-system-name>
 <routing-instance routing-instance-name>
```

Release Information

Description
Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options
bulk-leasequery-connections—(Optional) Display information about DHCPv6 local server bulk leasequery statistics.

logical-system logical-system-name—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

routing-instance routing-instance-name—(Optional) Display information about extended DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level
table view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>clear dhcpv6 server statistics</th>
<th>2474</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Client MAC Address Validation to Prevent Session Hijacking</td>
<td></td>
</tr>
</tbody>
</table>

List of Sample Output
show dhcpv6 server statistics on page 2638
show dhcpv6 server statistics bulk-leasequery-connections on page 2639

Output Fields
Table 78 on page 2637 lists the output fields for the `show dhcpv6 server statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 78: show dhcpv6 server statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets dropped</strong></td>
<td>Number of packets discarded by the extended DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total</strong>—Total number of packets discarded by the extended DHCPv6 local server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strict Reconfigure</strong>—Number of solicit messages discarded because the client does not support reconfiguration</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad hardware address</strong>—Number of packets discarded because an invalid hardware address was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad opcode</strong>—Number of packets discarded because an invalid operation code was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad options</strong>—Number of packets discarded because invalid options were specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client MAC validation</strong>—Number of packets discarded because validation of the client MAC address failed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid server address</strong>—Number of packets discarded because an invalid server address was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Lease Time Violation</strong>—Number of packets discarded because of a lease time violation</td>
</tr>
<tr>
<td></td>
<td>• <strong>No available addresses</strong>—Number of packets discarded because there were no addresses available for assignment</td>
</tr>
<tr>
<td></td>
<td>• <strong>No interface match</strong>—Number of packets discarded because they did not belong to a configured interface</td>
</tr>
<tr>
<td></td>
<td>• <strong>No routing instance match</strong>—Number of packets discarded because they did not belong to a configured routing instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>No valid local address</strong>—Number of packets discarded because there was no valid local address</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packet too short</strong>—Number of packets discarded because they were too short</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read error</strong>—Number of packets discarded because of a system read error</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send error</strong>—Number of packets that the extended DHCPv6 local server could not send</td>
</tr>
<tr>
<td><strong>Advertise Delay</strong></td>
<td>Number of DHCP advertise messages delayed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DELAYED</strong>—Number of DHCPv6 advertise packets that have been sent after being delayed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>INPROGRESS</strong>—Number of DHCPv6 advertise packets that are in the delay queue.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TOTAL</strong>—Total number of delayed DHCPv6 advertise messages; sum of <code>DELAYED</code> and <code>INPROGRESS</code>.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_CONFIRM</strong>—Number of DHCPv6 CONFIRM PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_DECLINE</strong>—Number of DHCPv6 DECLINE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_INFORMATION_REQUEST</strong>—Number of DHCPv6 INFORMATION-REQUEST PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_REBIND</strong>—Number of DHCPv6 REBIND PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RELAY_FORW</strong>—Number of DHCPv6 RELAY-FORW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RELAY_REPL</strong>—Number of DHCPv6 RELAY-REPL PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RELEASE</strong>—Number of DHCPv6 RELEASE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RENEW</strong>—Number of DHCPv6 RENEW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RENEW</strong>—Number of DHCPv6 REBIND PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_SOLICIT</strong>—Number of DHCPv6 SOLICIT PDUs received.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_LEASEQUERY</strong>—Number of DHCPv6 leasequery messages received.</td>
</tr>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCPv6 messages sent.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_ADVERTISE</strong>—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_REPLY</strong>—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_LOGICAL_NAK</strong>—Number of logical NAK messages sent, signifying T1 and T2 timers with values of zero; subset of <strong>DHCPv6_REPLY</strong> counter. (Displays only at <strong>verbose</strong> level.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RECONFIGURE</strong>—Number of DHCPv6 RECONFIGURE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RELAY_REPL</strong>—Number of DHCPv6 RELAY-REPL PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_RELAY_FORW</strong>—Number of DHCPv6 RELAY-FORW PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_LEASEQUERY_REPLY</strong>—Number of DHCPv6 leasequery replies transmitted to the DHCPv6 relay agent.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_LEASEQUERY_DATA</strong>—Number of DHCPv6 LEASEQUERY-DATA packets transmitted.</td>
</tr>
<tr>
<td></td>
<td>● <strong>DHCPv6_LEASEQUERY_DONE</strong>—Number of DHCPv6 LEASEQUERY-DONE packets sent.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show dhcpv6 server statistics

user@host> show dhcpv6 server statistics
```
Dhcpv6 Packets dropped:
  Total                      2
  Lease Time Violation       1
  Client MAC validation      1

Advertise Delay:
  DELAYED                    3
  INPROGRESS                 9
  TOTAL                     12

Messages received:
  DHCPV6_DECLINE             0
  DHCPV6_SOLICIT             9
  DHCPV6_INFORMATION_REQUEST 0
  DHCPV6_RELEASE             0
  DHCPV6_REQUEST             5
  DHCPV6_CONFIRM             0
  DHCPV6_RENEW               0
  DHCPV6_REBIND              0
  DHCPV6_RELAY_FORW          0

  DHCPV6_LEASEQUERY          0

Messages sent:
  DHCPV6_ADVERTISE           9
  DHCPV6_REPLY               5
  DHCPV6_RECONFIGURE         0
  DHCPV6_RELAY_REPL          0
  DHCPV6_LEASEQUERY_REPLY    0
  DHCPV6_LEASEQUERY_DATA     0
  DHCPV6_LEASEQUERY_DONE     0

show dhcpv6 server statistics bulk-leasequery-connections

user@host>  show dhcpv6 server statistics bulk-leasequery-connections

  Total Accepted Connections:                     0
  Total Not-Accepted Connections:                 0
  Connections Closed due to Errors:               0
  Connections Closed due to max-empty-replies:    0
  In-flight Connections:                          0
show dhcpv6 server statistics (View)

Syntax

```
show dhcpv6 server statistics
    <logical-system logical-system-name>
    <routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 10.4.

Description

Display DHCPv6 local server statistics.

Options

logical-system logical-system-name—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

routing-instance routing-instance-name—(Optional) Display information about DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege Level

view

RELATED DOCUMENTATION

| clear dhcpv6 server statistics (Local Server) | 2476 |

List of Sample Output

show dhcpv6 server statistics on page 2642

Output Fields

Table 79 on page 2641 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.
Table 79: show dhcpv6 server statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dhcpv6 Packets</td>
<td>Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td>dropped</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total number of packets discarded by the DHCPv6 local server</td>
</tr>
<tr>
<td>Authentication</td>
<td>Number of packets discarded because they could not be authenticated</td>
</tr>
<tr>
<td>Strict Reconfigure</td>
<td>Number of solicit messages discarded because the client does not support reconfiguration</td>
</tr>
<tr>
<td>Bad hardware address</td>
<td>Number of packets discarded because an invalid hardware address was specified</td>
</tr>
<tr>
<td>Bad opcode</td>
<td>Number of packets discarded because an invalid operation code was specified</td>
</tr>
<tr>
<td>Bad options</td>
<td>Number of packets discarded because invalid options were specified</td>
</tr>
<tr>
<td>Invalid server address</td>
<td>Number of packets discarded because an invalid server address was specified</td>
</tr>
<tr>
<td>No available addresses</td>
<td>Number of packets discarded because there were no addresses available for assignment</td>
</tr>
<tr>
<td>No interface match</td>
<td>Number of packets discarded because they did not belong to a configured interface</td>
</tr>
<tr>
<td>No routing instance match</td>
<td>Number of packets discarded because they did not belong to a configured routing instance</td>
</tr>
<tr>
<td>No valid local address</td>
<td>Number of packets discarded because there was no valid local address</td>
</tr>
<tr>
<td>Packet too short</td>
<td>Number of packets discarded because they were too short</td>
</tr>
<tr>
<td>Read error</td>
<td>Number of packets discarded because of a system read error</td>
</tr>
<tr>
<td>Send error</td>
<td>Number of packets that the DHCPv6 local server could not send</td>
</tr>
</tbody>
</table>
### Table 79: show dhcpv6 server statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_CONFIRM—Number of DHCPv6 CONFIRM PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_DECLINE—Number of DHCPv6 DECLINE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_INFORMATION_REQUEST—Number of DHCPv6 INFORMATION-REQUEST PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_REBIND—Number of DHCPv6 REBIND PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received from a relay by the</td>
</tr>
<tr>
<td></td>
<td>DHCPv6 server.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_RELEASE—Number of DHCPv6 RELEASE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_RENEW—Number of DHCPv6 RENEW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_REQUEST—Number of DHCPv6 REQUEST PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_SOLICIT—Number of DHCPv6 SOLICIT PDUs received.</td>
</tr>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCPv6 messages sent.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_REPLY—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>• DHCPv6_RELAY_REPL—Number of DHCPv6 RELAY_REPL PDUs sent from DHCPv6 server to</td>
</tr>
<tr>
<td></td>
<td>DHCPv6 relay.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show dhcpv6 server statistics
user@host> show dhcpv6 server statistics

Dhcpv6 Packets dropped:
  Total               0

Messages received:
  DHCPv6_DECLINE      0
  DHCPv6_SOLICIT      9
  DHCPv6_INFORMATION_REQUEST 0
  DHCPv6_RELEASE      0
  DHCPv6_REQUEST      5
  DHCPv6_CONFIRM      0
```
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6_RENEW</td>
<td>0</td>
</tr>
<tr>
<td>DHCPv6_REBIND</td>
<td>0</td>
</tr>
<tr>
<td>DHCPv6_RELAY_FORWARD</td>
<td>0</td>
</tr>
</tbody>
</table>

Messages sent:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6_ADVERTISE</td>
<td>9</td>
</tr>
<tr>
<td>DHCPv6_REPLY</td>
<td>5</td>
</tr>
<tr>
<td>DHCPv6_RECONFIGURE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPv6_RELAY_REPL</td>
<td>0</td>
</tr>
</tbody>
</table>
show dot1x

Syntax

```flexbox
show dot1x
  <brief | detail>
  <interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description

Display the current operational state of all ports with the list of connected users.

This command displays the list of connected supplicants received from the RADIUS authentication server regardless of the session state—that is, for both authenticated supplicants and for supplicants that attempted authentication.

Options

- **none**—Display information for all authenticator ports.
- **brief | detail**—(Optional) Display the specified level of output.
- **interface interface-name**—(Optional) Display information for the specified port with a list of connected supplicants.

Required Privilege Level

- view

RELATED DOCUMENTATION

- clear dot1x | 2477
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Example: Configuring 802.1X Authentication Options When the RADIUS Server Is Unavailable to an EX Series Switch | 408
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients | 415
List of Sample Output

*show dot1x interface brief on page 2649*
*show dot1x interface detail on page 2649*

Output Fields

Table 80 on page 2645 lists the output fields for the `show dot1x` command. Output fields are listed in the approximate order in which they appear.

Table 80: `show dot1x` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of a port.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the connected supplicant on the port.</td>
<td>All levels</td>
</tr>
<tr>
<td>Role</td>
<td>The 802.1X authentication role of the interface. When 802.1X is enabled on an interface, the role is <strong>Authenticator</strong>. As <strong>Authenticator</strong>, the interface blocks LAN access until a supplicant is authenticated through 802.1X or MAC RADIUS authentication.</td>
<td><strong>brief, detail</strong></td>
</tr>
</tbody>
</table>
| State      | The state of the port:  

  - **Authenticated**—The supplicant has been authenticated through the RADIUS server or has been permitted access through server fail fallback.  
  - **Authenticating**—The supplicant is authenticating through the RADIUS server.  
  - **Held**—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred. | **brief** |
| User       | The username of the connected supplicant. | **brief** |
Table 80: show dot1x Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| **Administrative state** | The administrative state of the port:  
  - **auto**—Traffic is allowed through the port based on the authentication result (by default).  
  - **force-authorize**—All traffic flows through the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to **dynamic**.  
  - **force-unauthorize**—All traffic drops on the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to **dynamic**. | detail          |
| **Suppliant**    | The mode for the supplicant:  
  - **single**—Only the first supplicant is authenticated. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication.  
  - **single-secure**—Only one supplicant is allowed to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out.  
  - **multiple**—Multiple supplicants are allowed to connect to the port. Each supplicant is authenticated individually. | detail          |
| **Quiet period** | The number of seconds the port waits following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds. | detail          |
| **Transmit period** | The number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant. The default value is 30 seconds. The range is 1 through 65,535 seconds. | detail          |
| **MAC radius**   | MAC RADIUS authentication:  
  - **enabled**—The switch sends an EAPOL request to the connecting host to attempt 802.1X authentication and if the connecting host is unresponsive, the switch tries to authenticate the host by using the MAC address.  
  - **disabled**—The default. The switch does not attempt to authenticate the MAC address of the connecting host. | detail          |
Table 80: show dot1x Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| **MAC radius authentication protocol** | MAC RADIUS authentication protocol:  
  - EAP-MD5—The EAP-MD5 protocol is used for MAC RADIUS authentication. EAP-MD5 is an authentication method belonging to the Extensible Authentication Protocol (EAP) authentication framework.  
  - PAP—The Password Authentication Protocol (PAP) authentication protocol is used for MAC RADIUS authentication.                                                                 | detail          |
| MAC radius restrict                | The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.                                                                                                                                                                      | detail          |
| Reauthentication                  | The reauthentication state:  
  - disable—Periodic reauthentication of the client is disabled.  
  - interval—Sets the periodic reauthentication time interval. The default value is 3600 seconds. The range is 1 through 65,535 seconds.                                                                                                                   | detail          |
| Supplicant timeout                | The number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request. The default value is 30 seconds. The range is 1 through 60 seconds.                                                                    | detail          |
| Server timeout                    | The number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out. The default value is 30 seconds. The range is 1 through 60 seconds.                                                                 | detail          |
| Maximum EAPOL requests            | The maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.                                                                 | detail          |
| Number of clients bypassed because of authentication | The number of non-802.1X clients granted access to the LAN by means of static MAC bypass. The following fields are displayed:  
  - Client—MAC address of the client.  
  - vlan—The name of the VLAN to which the client is connected.                                                                                                                                                    | detail          |
<p>| Guest VLAN member                 | The VLAN to which a supplicant is connected when the supplicant is authenticated using a guest VLAN. If a guest VLAN is not configured on the interface, this field displays &lt;not configured&gt;.                                                                 | detail          |
| Multi domain data session count   | The number of data sessions that have been authenticated on a multi-domain authentication interface.                                                                                                                                                    | detail          |</p>
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of connected supplicants</strong></td>
<td>The number of supplicants connected to a port.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Supplicant</strong></td>
<td>The username and MAC address of the connected supplicant.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Authentication method</strong></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td><strong>CWA Authentication</strong>—A supplicant is authenticated by the central Web authentication (CWA) server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Fail</strong>—Authentication failed and supplicant is in Held state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Guest VLAN</strong>—A supplicant is connected to the LAN through the guest VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MAC RADIUS</strong>—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RADIUS</strong>—A supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Server-fail</strong>—One of the following fallback actions is in effect because the RADIUS server is unreachable. Indicates whether EAPOL block is in effect, and the amount of time remaining for EAPOL block (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● <em>deny</em>—The supplicant is denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default server fail fallback action.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● <em>permit</em>—The supplicant is permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● <em>use-cache</em>—In the event that the RADIUS server times out when the supplicant is attempting reauthentication, the supplicant is reauthenticated only if it was previously authenticated; otherwise, the supplicant is denied LAN access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● <em>VLAN</em>—The supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● <em>Server-reject VLAN</em>—The supplicant received a RADIUS access-reject message from the authentication server and was moved to a server-reject VLAN, a specified VLAN already configured on the switch.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 80: show dot1x Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated VLAN</td>
<td>The VLAN to which the supplicant is connected.</td>
<td>detail</td>
</tr>
<tr>
<td>Dynamic filter</td>
<td>User policy filter sent by the RADIUS server.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Reauth interval</td>
<td>The configured reauthentication interval.</td>
<td>detail</td>
</tr>
<tr>
<td>Reauthentication due in</td>
<td>The number of seconds in which reauthentication will occur again for the connected supplicant.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Accounting Interim Interval</td>
<td>The number of seconds between interim RADIUS accounting messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Accounting Update due in</td>
<td>The number of seconds until the next interim RADIUS accounting update is due.</td>
<td>detail</td>
</tr>
<tr>
<td>CWA Redirect URL</td>
<td>The URL used to redirect the supplicant to a central Web server for authentication.</td>
<td>detail</td>
</tr>
<tr>
<td>Eapol Block</td>
<td>Shows whether EAPOL block is in effect or not in effect.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

**show dot1x interface brief**

```plaintext
user@switch> show dot1x interface brief

802.1X Information:
Interface   Role         State        MAC address         User
ge-0/0/1    Authenticator Authenticated 00:a0:d2:18:1a:c8   user1
ge-0/0/2    Authenticator Connecting 00:a0:b2:10:1a:c8     user1
ge-0/0/3    Authenticator Held         00:a6:55:f2:94:ae   user3
```

**show dot1x interface detail**

```plaintext
user@switch> show dot1x interface ge-0/0/16.0 detail
```
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Restrict: Disabled
  Mac Radius Authentication Protocol: PAP
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 2
    Supplicant: abc, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3587 seconds
      Eapol-Block: Not In Effect
    Supplicant: 000303030303, 00:03:03:03:03:03
      Operational state: Authenticated
      Backend Authentication state: Idle
      Authentication method: Mac Radius
      Authenticated VLAN: dyn_vlan2
      Session Reauth interval: 3600 seconds
      Reauthentication due in 3587 seconds
      Eapol-Block: In Effect
show dot1x accounting attribute

Syntax

```
show dot1x accounting attribute
```

Release Information

Command introduced in JUNOS Release 16.1 for EX Series switches.

Description

Display the RADIUS accounting attributes sent by the switch, operating as the network access server (NAS), to the RADIUS accounting server. RADIUS accounting attributes convey information that is used to account for a service provided to an authenticated user. The user session statistics are recorded by the accounting server in an accounting log file.

RADIUS accounting attributes are included in Accounting-Request messages sent from the switch to the accounting server. Attribute information is created only if the data for the attribute is available.

Required Privilege Level

view

RELATED DOCUMENTATION

- show dot1x | 2644
- clear dot1x | 2477
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479
- Example: Setting Up 802.1X for Single-Supplicant or Multiple-Supplicant Configurations on an EX Series Switch | 440
- Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395

List of Sample Output

show dot1x accounting-attributes on page 2652

Output Fields

Table 81 on page 2652 lists the output fields for the `show dot1x accounting-attributes` command. Output fields are listed in the approximate order in which they appear.
### Table 81: show dot1x accounting attribute Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting attributes</td>
<td>Shows the value for the RADIUS accounting attributes sent from the NAS to the server. An attribute is displayed only if data is available for that attribute value. The following RADIUS accounting attributes are supported:</td>
</tr>
<tr>
<td></td>
<td>• User-Name—The name of the authenticated user.</td>
</tr>
<tr>
<td></td>
<td>• NAS-Port—The physical port number of the NAS which is authenticating the user.</td>
</tr>
<tr>
<td></td>
<td>• Framed-IP-Address—The IP address of the authenticated user.</td>
</tr>
<tr>
<td></td>
<td>• Filter-ID—The name of the filter list for the authenticated user.</td>
</tr>
<tr>
<td></td>
<td>• Framed-MTU—The maximum transmission unit that can be configured for user.</td>
</tr>
<tr>
<td></td>
<td>• Client-System-Name—This is a vendor-specific attribute (VSA) used to indicate the client host name. Supported for LLDP-capable devices only.</td>
</tr>
<tr>
<td></td>
<td>• Session-Timeout—The maximum number of seconds that a session will stay active before termination of the session or prompt.</td>
</tr>
<tr>
<td></td>
<td>• Called-Station-ID—Allows the NAS to send the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology.</td>
</tr>
<tr>
<td></td>
<td>• Calling-Station-ID—Allows the NAS to send the phone number that the call came from, using Dialed Number Identification (DNIS) or similar technology.</td>
</tr>
<tr>
<td></td>
<td>• NAS-Identifier—Contains a string identifying the NAS originating the Accounting-Request.</td>
</tr>
<tr>
<td></td>
<td>• Acct-Status-Type—Indicates whether this Accounting-Request marks the beginning of the user session (Start) or the end (Stop). Can also be used for an interim update (Interim-Update).</td>
</tr>
<tr>
<td></td>
<td>• Acct-Authentic—Indicates whether the user was authenticated locally (Local), by the RADIUS server (RADIUS), or by another remote authentication protocol (Remote).</td>
</tr>
<tr>
<td></td>
<td>• Acct-Session-ID—A unique ID for a specific accounting session that can be used to match start and stop records for a session in the log file.</td>
</tr>
<tr>
<td></td>
<td>• Event-Timestamp—Records the time an event occurred.</td>
</tr>
<tr>
<td></td>
<td>• NAS-Port-ID—The port of the NAS that is authenticating the user.</td>
</tr>
<tr>
<td></td>
<td>• Framed-IPv6-Address—The IPv6 address of the authenticated user.</td>
</tr>
</tbody>
</table>

---

### Sample Output

**show dot1x accounting-attributes**

user@switch> **show dot1x accounting-attributes**

Accounting Attribute:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Station Id:</td>
<td>88-e0-f3-1f-c5-e0</td>
</tr>
<tr>
<td>Called station Id:</td>
<td>00-10-94-00-00-02</td>
</tr>
<tr>
<td>Framed Ipv6 Address:</td>
<td>:2001:db8:0:1:2a0:a514:0:24d</td>
</tr>
<tr>
<td>Accounting Session ID:</td>
<td>802.1x812f00250002dccc6</td>
</tr>
<tr>
<td>Client System Name:</td>
<td>AVX149485</td>
</tr>
<tr>
<td>Session-Timeout:</td>
<td>120s</td>
</tr>
<tr>
<td>Framed-MTU:</td>
<td>492</td>
</tr>
<tr>
<td>Acct-Authentic:</td>
<td>RADIUS</td>
</tr>
<tr>
<td>Nas-Port-ID</td>
<td>ge-0/0/5.0</td>
</tr>
</tbody>
</table>
show dot1x authentication-failed-users

Syntax

```plaintext
show dot1x authentication-failed-users
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description
Display the supplicants (users) that have failed 802.1X authentication.

Required Privilege Level
view

RELATED DOCUMENTATION
- clear dot1x | 2477
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479
- Configuring 802.1X Interface Settings (CLI Procedure) | 390

List of Sample Output
show dot1x authentication-failed-users on page 2655

Output Fields
Table 82 on page 2654 lists the output fields for the `show dot1x authentication-failed-users` command. Output fields are listed in the approximate order in which they appear.

Table 82: show dot1x authentication-failed-users Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MAC address configured to bypass 802.1X authentication.</td>
<td>all</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address configured statically on the interface.</td>
<td>all</td>
</tr>
<tr>
<td>User</td>
<td>The user that is configured on the RADIUS server and that has failed 802.1X authentication.</td>
<td>all</td>
</tr>
</tbody>
</table>
Table 82: show dot1x authentication-failed-users Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Count</td>
<td>The number of times that 802.1X authentication has failed on the interface.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

```
show dot1x authentication-failed-users

user@switch> show dot1x authentication-failed-users

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC address</th>
<th>User</th>
<th>Failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/17.0</td>
<td>00:37:00:00:00:00</td>
<td>003700000000</td>
<td>28</td>
</tr>
<tr>
<td>ge-0/0/20.0</td>
<td>00:04:10:00:00:00</td>
<td>000410000000</td>
<td>32</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>00:00:03:00:0a:00</td>
<td>000003000a00</td>
<td>4</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>00:00:03:00:0b:00</td>
<td>000003000b00</td>
<td>18</td>
</tr>
</tbody>
</table>
```
show dot1x firewall

Syntax

```
show dot1x firewall <interface interface-name>
```

Release Information
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

Description
Display information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user.

Options

none—Display information for all interfaces.

interface interface-names—(Optional) Display information for the specified interface.

Required Privilege Level

view

RELATED DOCUMENTATION

| clear dot1x | 2477 |

List of Sample Output

show dot1x firewall on page 2656
show dot1x firewall on page 2657

Output Fields

Output fields include any action modifier that is specified in firewall filters.

Sample Output

```
show dot1x firewall
(Showing counter action)
```
user@switch> **show dot1x firewall**

Filter: dot1x-filter-ge-0/0/3
Counters
  counter1_dot1x_ge-0/0/3_user1   342
  counter1_dot1x_ge-0/0/3_user2   857

**show dot1x firewall**
(Showing policer action)

user@switch> **show dot1x firewall**

Filter: dot1x_ge-0/0/0
Counters
  pl-t1    494946
**show dot1x static-mac-address**

**Syntax**

```
show dot1x static-mac-address <(interface [interface-name])>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Command introduced in Junos OS Release 14.2 for MX240, MX480, and MX960 routers in enhanced LAN mode.

**Description**
Display all the static MAC addresses that are configured to bypass 802.1X authentication on the switch.

**Options**

- **none**—Display static MAC addresses for all interfaces.

- **interface interface-name**—(Optional) Display static MAC addresses for a specific interface.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**

- clear dot1x | 2477
- Example: Configuring Static MAC Bypass of 802.1X and MAC RADIUS Authentication on an EX Series Switch | 479
- Adding a Static MAC Address Entry to the Ethernet Switching Table on a Switch with ELS Support
- Configuring 802.1X Interface Settings (CLI Procedure) | 390
- Understanding Authentication on Switches | 361

**List of Sample Output**

- show dot1x static-mac-address on page 2659
- show dot1x static-mac-address interface (Specific Interface) on page 2659

**Output Fields**

Table 83 on page 2659 lists the output fields for the **show dot1x static-mac-address** command. Output fields are listed in the approximate order in which they appear.
### Table 83: show dot1x static-mac-address Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>The MAC address of the device that is configured to bypass 802.1X authentication.</td>
<td>all</td>
</tr>
<tr>
<td>VLAN-Assignment</td>
<td>The name of the VLAN to which the device is assigned.</td>
<td>all</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the interface on which authentication is bypassed for a given MAC address.</td>
<td>all</td>
</tr>
</tbody>
</table>

### Sample Output

**show dot1x static-mac-address**

```
user@switch>   show dot1x static-mac-address

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:11:22:33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:00:12:12</td>
<td>ge-0/0/3.0</td>
<td></td>
</tr>
<tr>
<td>00:00:02:34:56</td>
<td>facilities</td>
<td>ge-0/0/1.0</td>
</tr>
</tbody>
</table>
```

**show dot1x static-mac-address interface (Specific Interface)**

```
user@switch>   show dot1x static-mac-address interface ge-0/0/0.1

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:12:24:12</td>
<td>support</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>00:00:00:72:30:58</td>
<td>support</td>
<td>ge-0/0/1.0</td>
</tr>
</tbody>
</table>
```
show dot1x statistics

Syntax

show dot1x statistics
<interface interface>

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the number of EAPOL messages transmitted or received on all interfaces or specific interfaces.

Options

none—Displays statistical information for all interfaces.

interface interface-name—(Optional) Displays statistical information for the specified interface.

Required Privilege Level
view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>show dot1x</th>
<th>2644</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear dot1x</td>
<td>2477</td>
</tr>
</tbody>
</table>

Example: Setting Up 802.1X for Single-Suppliant or Multiple-Suppliant Configurations on an EX Series Switch | 440
Filtering 802.1X Supplicants by Using RADIUS Server Attributes | 395

List of Sample Output

show dot1x statistics interface on page 2661

Output Fields

Table 81 on page 2652 lists the output fields for the show dot1x statistics command. Output fields are listed in the approximate order in which they appear.

Table 84: show dot1x statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxReqId</td>
<td>The number of EAP-Request/Identity messages transmitted on the interface.</td>
</tr>
</tbody>
</table>
Table 84: show dot1x statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxReq</td>
<td>The number of transmitted EAP-Request frames that were not EAP-Request/Identity.</td>
</tr>
<tr>
<td>TxTotal</td>
<td>The total number of EAPOL messages transmitted on the interface.</td>
</tr>
<tr>
<td>RxStart</td>
<td>The number of EAPOL-Start messages received on the interface.</td>
</tr>
<tr>
<td>RxLogoff</td>
<td>The number of EAP-Logoff messages received on the interface.</td>
</tr>
<tr>
<td>RxRespld</td>
<td>The number of EAP-Response/Identity frames received on the interface.</td>
</tr>
<tr>
<td>RxResp</td>
<td>The number of EAP-Response messages received that were not EAP-Response/Identity.</td>
</tr>
<tr>
<td>CoA-Request</td>
<td>The number of Change of Authorization (CoA) Request messages received on the interface.</td>
</tr>
<tr>
<td>CoA-Ack</td>
<td>The number of CoA-Ack messages transmitted on the interface.</td>
</tr>
<tr>
<td>CoA-Nak</td>
<td>The number of CoA-Nak messages transmitted on the interface.</td>
</tr>
<tr>
<td>RxInvalid</td>
<td>The number of invalid EAPOL messages received on the interface.</td>
</tr>
<tr>
<td>RxLenErr</td>
<td>The number of EAPOL messages with incorrect length received on the interface.</td>
</tr>
<tr>
<td>RxTotal</td>
<td>The total number of EAPOL messages received on the interface.</td>
</tr>
<tr>
<td>LastRxVersion</td>
<td>The version number of the last EAPOL message received on the interface.</td>
</tr>
<tr>
<td>LastRxSrcMac</td>
<td>The source MAC address in the last EAPOL message received on the interface.</td>
</tr>
<tr>
<td>PortBounceReqRx</td>
<td>The number of port bounce requests received on the port.</td>
</tr>
</tbody>
</table>

Sample Output

```
show dot1x statistics interface
user@host> show dot1x statistics interface ge-0/0/0

Interface: ge-0/0/0.0
  TxReqId = 4  TxReq = 0  TxTotal = 4
```
RxStart = 0  RxLogoff = 0  RxRespId = 0  RxResp = 0
CoA-Request = 0  CoA-Ack = 0  CoA-Nak = 0
RxInvalid = 0  RxLenErr = 0  RxTotal = 0
LastRxVersion = 0  LastRxSrcMac = 00:50:56:85:66:0f
PortBounceReqRx = 0
show ethernet-switching interface

Syntax

```
show ethernet-switching interface
<brief | detail | extensive>
<interface-name>
```

Release Information
Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Command introduced in Junos OS Release 13.2x51 for QFX Series switches.

Description
Display Layer 2 learning information for all the interfaces.

Options
none—Display Ethernet-switching information for all interfaces.

brief | detail | extensive—(Optional) Display the specified level of output.

interface-name—(Optional) Display Ethernet-switching information for the specified interface.

Required Privilege Level
view

RELATED DOCUMENTATION

List of Sample Output
show ethernet switching interface (Specific Interface) on page 2664
show ethernet-switching interface detail on page 2665

Output Fields
Table 85 on page 2663 describes the output fields for the show ethernet-switching interface command. Output fields are listed in the approximate order in which they appear.

Table 85: show ethernet-switching interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>VLAN members</td>
<td>VLANs associated with this interface.</td>
</tr>
</tbody>
</table>
### Table 85: show ethernet-switching interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag</td>
<td>VLAN ID.</td>
</tr>
<tr>
<td>MAC limit</td>
<td>Number of MAC addresses that can be associated with the interface.</td>
</tr>
<tr>
<td>STP state</td>
<td>Spanning Tree protocol (STP) state.</td>
</tr>
<tr>
<td>Logical interface flags</td>
<td>Status of Layer 2 learning properties for each interface:</td>
</tr>
<tr>
<td></td>
<td>• DL—MAC learning is disabled.</td>
</tr>
<tr>
<td></td>
<td>• LH—MAC interface limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>• AD—Packets are dropped after the MAC interface limit is reached.</td>
</tr>
<tr>
<td></td>
<td>• DN—The MAC interface is down.</td>
</tr>
<tr>
<td></td>
<td>• MMAS—The MAC interface is disabled after a MAC address move.</td>
</tr>
<tr>
<td></td>
<td>• SCTL—The MAC interface is disabled after a configured storm-control level is exceeded.</td>
</tr>
<tr>
<td>Tagging</td>
<td>Tagging state of the VLAN.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ethernet switching interface (Specific Interface)**

```bash
user@host> show ethernet-switching interface ae10.0
```

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Vlan members</th>
<th>TAG</th>
<th>MAC limit</th>
<th>STP state</th>
<th>Logical interface flags</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae10.0</td>
<td>VLAN70..</td>
<td>701</td>
<td>1024</td>
<td>Forwarding</td>
<td>tagged</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN70..</td>
<td>702</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN70..</td>
<td>703</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)
show ethernet-switching interface detail
user@host>  show ethernet-switching interface detail

Information for interface family:
Name: ge-1/0/3.0
  Type: IFF                 Handle: 0x8bba280
  Index: 331                Generation: 159
  Flags: UP,
  IFD index: 141            Routing/Vlan index: 4
  IFL index: 331            Address family: 50
  Sequence number: 0        MAC sequence number: 0
  MAC limit: 65535          MACs learned: 0
  Static MACs learned: 0    Non configured static MACs learned: 0
Name: ge-1/0/3.0
  Type: IFBD (static)       Handle: 0x8bb6e00
  Index:                     Generation: 129
  Trunk id: 0                Flags: UP,
<table>
<thead>
<tr>
<th>IFD index:</th>
<th>Routing/Vlan index: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFL index:</td>
<td>Address family:</td>
</tr>
<tr>
<td>Sequence number: 1</td>
<td>MAC sequence number: 1</td>
</tr>
<tr>
<td>MAC limit: 65535</td>
<td>MACs learned: 0</td>
</tr>
<tr>
<td>Static MACs learned: 0</td>
<td>Non configured static MACs learned: 0</td>
</tr>
<tr>
<td>VSTP index: 11</td>
<td>Rewrite op:</td>
</tr>
<tr>
<td>Name: ge-1/0/3.0</td>
<td></td>
</tr>
<tr>
<td>Type: IFBD (static)</td>
<td>Handle: 0x8bb6f00</td>
</tr>
<tr>
<td>Index:</td>
<td>Generation: 130</td>
</tr>
<tr>
<td>Trunk id: 0</td>
<td>Flags: UP,</td>
</tr>
<tr>
<td>IFD index:</td>
<td></td>
</tr>
<tr>
<td>IFL index:</td>
<td>Routing/Vlan index: 3</td>
</tr>
<tr>
<td>Sequence number: 1</td>
<td>MAC sequence number: 1</td>
</tr>
<tr>
<td>MAC limit: 65535</td>
<td>MACs learned: 0</td>
</tr>
<tr>
<td>Static MACs learned: 0</td>
<td>Non configured static MACs learned: 0</td>
</tr>
<tr>
<td>VSTP index: 11</td>
<td>Rewrite op:</td>
</tr>
</tbody>
</table>
show ethernet-switching interfaces

Syntax

```
show ethernet-switching interfaces
  <brief | detail | summary>
  <interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
In Junos OS Release 9.6 for EX Series switches, the following updates were made:

- **Blocking** field output was updated.
- The default view was updated to include information about 802.1Q tags.
- The **detail** view was updated to include information on VLAN mapping.

Command introduced in Junos OS Release 11.1 for the QFX Series.
In Junos OS Release 11.1 for EX Series switches, the **detail** view was updated to include reflective relay information.

Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description

Display information about switched Ethernet interfaces.

Options

- **none**—(Optional) Display brief information for Ethernet-switching interfaces.
- **brief | detail | summary**—(Optional) Display the specified level of output.
- **interface interface-name**—(Optional) Display Ethernet-switching information for a specific interface.

Required Privilege Level

- **view**

RELATED DOCUMENTATION

- Troubleshooting Ethernet Switching
- Understanding Bridging and VLANs on Switches
- Example: Setting Up Basic Bridging and a VLAN on Switches
- Example: Setting Up Bridging with Multiple VLANs
- Understanding FCoE
Interfaces Overview for Switches

-show ethernet-switching mac-learning-log
-show ethernet-switching table

Configuring Autorecovery for Port Security Events

List of Sample Output
-show ethernet-switching interfaces on page 2671
-show ethernet-switching interfaces summary on page 2672
-show ethernet-switching interfaces brief on page 2672
-show ethernet-switching interfaces detail on page 2672
-show ethernet-switching interfaces interface-name on page 2673
-show ethernet-switching interfaces on page 2674
-show ethernet-switching interfaces ge-0/0/15 brief on page 2674
-show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup) on page 2674
-show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP) on page 2675
-show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control) on page 2675
-show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping) on page 2675
-show ethernet-switching interfaces detail (Reflective Relay Is Configured) on page 2675

Output Fields

For QFX Series, QFabric, NFX Series, EX4600 and OCX1100:

Table 86 on page 2668 lists the output fields for the `show ethernet-switching interfaces` command on QFX Series, QFabric, NFX Series, EX4600 and OCX1100. Output fields are listed in the approximate order in which they appear.

Table 86: show ethernet-switching interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of a switching interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>Interface state. Values are up or down.</td>
<td>none, brief, detail,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary</td>
</tr>
<tr>
<td>VLAN members</td>
<td>Name of a VLAN.</td>
<td>none, brief, detail,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary</td>
</tr>
</tbody>
</table>
Table 86: show ethernet-switching interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking</td>
<td>Forwarding state of the interface:</td>
<td>none, brief, detail, summary</td>
</tr>
<tr>
<td></td>
<td>• blocked—Traffic is not being forwarded on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unblocked—Traffic is forwarded on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC limit exceeded—The interface is temporarily disabled because of a MAC limiting error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC move limit exceeded—The interface is temporarily disabled because of a MAC move limiting error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Storm control in effect —The interface is temporarily disabled because of a storm control error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Storm control shutdown in effect —The interface is temporarily disabled because of a storm control shutdown error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>VLAN index internal to Junos OS software.</td>
<td>detail</td>
</tr>
<tr>
<td>untagged</td>
<td>tagged</td>
<td>Specifies whether the interface forwards IEEE802.1Q-tagged or untagged traffic.</td>
</tr>
</tbody>
</table>

Output fields for EX Series:

Table 87 on page 2669 lists the output fields for the show ethernet-switching interfaces command on EX Series switches. Output fields are listed in the approximate order in which they appear.

Table 87: show ethernet-switching interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of a switching interface.</td>
<td>none, brief, detail, summary</td>
</tr>
<tr>
<td>Index</td>
<td>VLAN index internal to Junos OS.</td>
<td>detail</td>
</tr>
<tr>
<td>State</td>
<td>Interface state. Values are up and down.</td>
<td>none, brief, detail</td>
</tr>
<tr>
<td>Port mode</td>
<td>The access mode is the port mode default and works with a single VLAN. Port mode can also be trunk, which accepts tagged packets from multiple VLANs on other switches. The third port mode value is tagged-access, which accepts tagged packets from access devices.</td>
<td>detail</td>
</tr>
</tbody>
</table>
### Table 87: show ethernet-switching interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflective Relay</td>
<td>Reflective relay allows packets to use the same interface for both upstream and downstream traffic. When reflective relay has been configured, the status displayed is always <strong>enabled</strong>. When reflective relay is not configured, this entry does not appear in the command output.</td>
<td>detail</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ether type for the</td>
<td>Ether type is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of an incoming Ethernet packet. Both 802.1Q packets and Q-in-Q packets use this field. The output displayed for this particular field indicates the interface's Ether type, which is used to match the Ether type of incoming 802.1Q packets and Q-in-Q packets. The indicated Ether type field is also added to the interface's outgoing 802.1Q and Q-in-Q packets.</td>
<td>detail</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN membership</td>
<td>Names of VLANs that belong to this interface.</td>
<td>none, brief, detail</td>
</tr>
<tr>
<td>Tag</td>
<td>Number of the 802.1Q tag.</td>
<td>none, brief, detail</td>
</tr>
<tr>
<td>Tagging</td>
<td>Specifies whether the interface forwards 802.1Q <strong>tagged</strong> or <strong>untagged</strong> traffic.</td>
<td>none, brief, detail</td>
</tr>
<tr>
<td>Blocking</td>
<td>The forwarding state of the interface:</td>
<td>none, brief, detail</td>
</tr>
<tr>
<td></td>
<td>• unblocked—Traffic is forwarded on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• blocked—Traffic is not being forwarded on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled by bpdu control—The interface is disabled due to receiving BPDUs on a protected interface. If the <strong>disable-timeout</strong> statement has been included in the BPDU configuration, the interface automatically returns to service after the timer expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• blocked by RTG—The specified redundant trunk group is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• blocked by STP—The interface is disabled due to a spanning-tree protocol error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC limit exceeded—The interface is temporarily disabled due to a MAC limit error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC move limit exceeded—The interface is temporarily disabled due to a MAC move limit error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Storm control in effect—The interface is temporarily disabled due to a storm control error. The disabled interface is automatically restored to service when the disable timeout expires.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 87: show ethernet-switching interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of MACs learned on IFL</td>
<td>Number of MAC addresses learned by this interface.</td>
<td>detail</td>
</tr>
<tr>
<td>mapping</td>
<td>When mapping is configured, the status is one of the following C-VLAN to S-VLAN mapping types:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>dot1q-tunneled</strong>—The interface maps all traffic to the S-VLAN (all-in-one bundling).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>native</strong>—The interface maps untagged and priority tagged packets to the S-VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>push</strong>—The interface maps packets to a firewall filter to an S-VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>policy-mapped</strong>—The interface maps packets to a specifically defined S-VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>integer</strong>—The interface maps packets to the specified S-VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When mapping is not configured, this entry does not appear in the command output.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Sample Output for QFX Series Switches, QFabric, NFX Series, EX4600 and OCX1100**

```
show ethernet-switching interfaces

user@switch> show ethernet-switching interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-0/0/0.0</td>
<td>up</td>
<td>T122</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/1.0</td>
<td>down</td>
<td>default</td>
<td>- MAC limit exceeded</td>
</tr>
<tr>
<td>xe-0/0/2.0</td>
<td>down</td>
<td>default</td>
<td>- MAC move limit exceeded</td>
</tr>
<tr>
<td>xe-0/0/3.0</td>
<td>down</td>
<td>default</td>
<td>- Storm control in effect</td>
</tr>
<tr>
<td>xe-0/0/4.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/5.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/6.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/7.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/8.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/9.0</td>
<td>up</td>
<td>T111</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/11.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
</tbody>
</table>
```
show ethernet-switching interfaces summary

user@switch>  show ethernet-switching interfaces summary

xe-0/0/0.0
xe-0/0/1.0
xe-0/0/2.0
xe-0/0/3.0
xe-0/0/8.0
xe-0/0/10.0
xe-0/0/11.0

show ethernet-switching interfaces brief

user@switch>  show ethernet-switching interfaces brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-0/0/0.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/1.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/2.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/3.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/8.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>xe-0/0/11.0</td>
<td>down</td>
<td>employee-vlan</td>
<td>unblocked</td>
</tr>
</tbody>
</table>

show ethernet-switching interfaces detail

user@switch>  show ethernet-switching interfaces detail
show ethernet-switching interfaces interface-name

user@switch> show ethernet-switching interfaces xe-0/0/0.0

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-0/0/0.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
</tbody>
</table>
Sample Output for EX Series Switches

show ethernet-switching interfaces

user@switch> show ethernet-switching interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Tag</th>
<th>Tagging</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae0.0</td>
<td>up</td>
<td>default</td>
<td></td>
<td></td>
<td>untagged, unblocked</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>up</td>
<td>vlan300</td>
<td>300</td>
<td>untagged</td>
<td>blocked by RTG (rtggroup)</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>up</td>
<td>default</td>
<td></td>
<td></td>
<td>blocked by STP</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>down</td>
<td>default</td>
<td></td>
<td></td>
<td>MAC limit exceeded</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>down</td>
<td>default</td>
<td></td>
<td></td>
<td>MAC move limit exceeded</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>down</td>
<td>default</td>
<td></td>
<td></td>
<td>Storm control in effect</td>
</tr>
<tr>
<td>ge-0/0/7.0</td>
<td>down</td>
<td>default</td>
<td></td>
<td></td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/13.0</td>
<td>up</td>
<td>default</td>
<td></td>
<td></td>
<td>untagged, unblocked</td>
</tr>
<tr>
<td>ge-0/0/14.0</td>
<td>up</td>
<td>vlan100</td>
<td>100</td>
<td>tagged</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/15.0</td>
<td>up</td>
<td>vlan100</td>
<td>100</td>
<td>tagged</td>
<td>blocked by STP</td>
</tr>
<tr>
<td>ge-0/0/16.0</td>
<td>down</td>
<td>default</td>
<td></td>
<td></td>
<td>untagged, unblocked</td>
</tr>
<tr>
<td>ge-0/0/17.0</td>
<td>down</td>
<td>vlan100</td>
<td>100</td>
<td>tagged</td>
<td>Disabled by bpdu-control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan200</td>
<td>200</td>
<td>tagged</td>
<td>Disabled by bpdu-control</td>
</tr>
</tbody>
</table>

show ethernet-switching interfaces ge-0/0/15 brief

user@switch> show ethernet-switching interfaces ge-0/0/15 brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Tag</th>
<th>Tagging</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/15.0</td>
<td>up</td>
<td>vlan100</td>
<td>100</td>
<td>tagged</td>
<td>blocked by STP</td>
</tr>
<tr>
<td>ge-0/0/15.0</td>
<td>up</td>
<td>vlan200</td>
<td>200</td>
<td>tagged</td>
<td>blocked by STP</td>
</tr>
</tbody>
</table>

show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup)

user@switch> show ethernet-switching interfaces ge-0/0/2 detail

Interface: ge-0/0/2.0, Index: 65, State: up, Port mode: Access
Ether type for the interface: 0x8100
VLAN membership:
  vlan300, 802.1Q Tag: 300, untagged, msti-id: 0, blocked by RTG(rtggroup)
show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP)

Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
  vlan100, 802.1Q Tag: 100, tagged, msti-id: 0, blocked by STP
  vlan200, 802.1Q Tag: 200, tagged, msti-id: 0, blocked by STP

Number of MACs learned on IFL: 0

show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control)

Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
Ether type for the interface: 0X8100
VLAN membership:
  vlan100, 802.1Q Tag: 100, tagged, msti-id: 1, Disabled by bpdu-control
  vlan200, 802.1Q Tag: 200, tagged, msti-id: 2, Disabled by bpdu-control

Number of MACs learned on IFL: 0

show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping)

Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
  map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
  map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked

show ethernet-switching interfaces detail (Reflective Relay Is Configured)

Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
Ether type for the interface: 0X8100
VLAN membership:
  map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
  map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked
Interface: ge-7/0/2, Index: 66, State: down, Port mode: Tagged-access
Ether type for the interface: 0x8100
Reflective Relay Status: Enabled
Ether type for the interface: 0x8100
VLAN membership:
  VLAN_Purple VLAN_Orange VLAN_Blue, 802.1Q Tag: 450, tagged, unblocked
Number of MACs learned on IFL: 0
show firewall (View)

Syntax

```
show firewall
<filter filter-name>
<counter counter-name>
<log>
<prefix-action-stats>
<terse>
```

Release Information
Command introduced before Junos OS Release 10.0.

Description
Display statistics about configured firewall filters.

Options
- **none**—Display statistics about configured firewall filters.
- **filter filter-name**—Name of a configured filter.
- **counter counter-name**—Name of a filter counter.
- **log**—Display log entries for firewall filters.
- **prefix-action-stats**—Display prefix action statistics for firewall filters.
- **terse**—Display firewall filter names only.

Required Privilege Level
view

RELATED DOCUMENTATION

| firewall | 1153 |

List of Sample Output
**show firewall on page 2678**

Output Fields
**Table 88 on page 2678** lists the output fields for the `show firewall` command. Output fields are listed in the approximate order in which they appear.
### Table 88: show firewall Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter</strong></td>
<td>Name of a filter that has been configured with the <code>filter</code> at the <code>[edit firewall]</code> hierarchy level. When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either <code>-i</code> for an input filter or <code>-o</code> for an output filter. When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either <code>-in</code> for an input filter or <code>-out</code> for an output filter. When a logical system–specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, <code>__ls1/filter1</code>).</td>
</tr>
<tr>
<td><strong>Counters</strong></td>
<td>Display filter counter information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Name of a filter counter that has been configured with the <code>counter</code> firewall filter action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—Number of bytes that match the filter term under which the <code>counter</code> action is specified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets that matched the filter term under which the <code>counter</code> action is specified.</td>
</tr>
<tr>
<td><strong>Policers</strong></td>
<td>Display policer information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Name of policer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show firewall
user@host> show firewall

Filter: ef_path
Counters:
Name            Bytes  Packets
def-count       0       0
video-count     0       0
```
<table>
<thead>
<tr>
<th>Filter: <strong>default_bpdu_filter</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>voice-count</strong></td>
</tr>
</tbody>
</table>

**Filter: deep**

Counters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>deep2</td>
<td>302076</td>
<td>5031</td>
</tr>
</tbody>
</table>

**Filter: deep-flood**

Counters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>deep_flood_def</td>
<td>302136</td>
<td>5032</td>
</tr>
<tr>
<td>deep1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Policers:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>deep-pol-op-first</td>
<td>0</td>
</tr>
</tbody>
</table>
show lldp

Syntax

```plaintext
show lldp
<detail>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol–Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.

NOTE: LLDP-MED is not available on the QFX Series.

Options

- `none`—Display LLDP information for all interfaces.
- `detail`—(Optional) Display detailed LLDP information for all interfaces.

Required Privilege Level

- `view`

RELATED DOCUMENTATION

- Configuring LLDP (CLI Procedure) | 654
- Configuring LLDP-MED (CLI Procedure) | 665
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
- Understanding LLDP | 653

List of Sample Output

- show lldp (EX3200 switches) on page 2685
- show lldp (EX4300 switches) on page 2685
Output Fields

Table 89 on page 2681 lists the output fields for the `show lldp` command. Output fields are listed in the approximate order in which they appear.

Table 89: show lldp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>LLDP operating state. The state can be <strong>enabled</strong> or <strong>disabled</strong>. <strong>NOTE:</strong> If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>Frequency, in seconds, at which LLDP advertisements are sent. This value is set by the <code>advertisement-interval</code> configuration statement.</td>
<td>All levels</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system. This value is set by the <code>transmit-delay</code> configuration statement.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold timer</td>
<td>On EX4300 switches, the hold timer shows the length of time LLDP information is held before it is discarded. The hold timer value is equal to the advertisement interval multiplied by the hold multiplier. On all other switches, the hold timer shows the value of the hold multiplier. The hold multiplier value is set by the <code>hold-multiplier</code> configuration statement.</td>
<td>All levels</td>
</tr>
<tr>
<td>Notification interval</td>
<td>How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications on database changes are disabled. This value is set by the <code>lldp-configuration-notification-interval</code> configuration statement.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 89: show lldp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Config Trap Interval</strong></td>
<td>How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications on topology changes are disabled. This value is set by the <code>ptopo-configuration-trap-interval</code> configuration statement.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Connection Hold timer</strong></td>
<td>Amount of time the system maintains dynamic topology entries. This value is set by the <code>ptopo-configuration-maximum-hold-time</code> configuration statement.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>LLDP-MED</strong></td>
<td>LLDP-MED operating state. The state can be <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MED fast start count</strong></td>
<td>Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second. This value is set by using the <code>fast-start</code> configuration statement. <strong>NOTE:</strong> <code>fast-start</code> is not available on the QFX Series.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Name of the interface for which LLDP configuration information is being reported.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>LLDP</strong></td>
<td>LLDP operating state. The state can be <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Power Negotiation</strong></td>
<td>LLDP power negotiation operating state. The state can be <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Neighbor count</strong></td>
<td>Total number of new LLDP neighbors detected since the last switch reboot. <strong>detail</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Name of the interface that is advertising VLAN information.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Vlan-id</strong></td>
<td>VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0. <strong>detail</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Table 89: show lldp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-name</td>
<td>VLAN name associated with the VLAN ID. For switches running Junos OS releases with Enhanced Layer 2 Software (ELS), this column displays the string <code>vlan-vlan-id</code> by default. Starting in Junos OS Release 15.1X53-D59 and 18.2R1, you can configure the <code>vlan-name-tlv-option name</code> option at the [edit protocols lldp] hierarchy level to transmit the VLAN name in the LLDP VLAN name TLV in place of the VLAN ID, and display the actual VLAN name in this output field instead.</td>
<td>detail</td>
</tr>
</tbody>
</table>
| LLDP basic TLVs supported | Basic TLVs supported on the switch:  
- **Chassis identifier**—TLV that advertises the MAC address associated with the local system.  
- **Port identifier**—TLV that advertises the port identification for the specified port in the local system.  
- **Port description**—Interface name for the port.  
- **System name**—TLV that advertises the user-configured name of the local system.  
- **System description**—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable.  
- **System capabilities**—TLV that advertises the primary functions performed by the system—for example, bridge or router.  
- **Management address**—TLV that advertises the IP management address of the local system. | detail |
### Supported LLDP 802 TLVs

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported LLDP 802 TLVs</strong></td>
<td>802.3 TLVs supported on the switch:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC/PHY configuration status</strong>—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Power via MDI</strong>—TLV that advertises MDI power support, PSE power pair, and power class information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link aggregation</strong>—TLV that advertises if the interface is aggregated and its aggregated interface ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum frame size</strong>—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port VLAN tag</strong>—TLV that advertises the VLAN tag configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port VLAN name</strong>—TLV that advertises the VLAN name configured on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

### Supported LLDP MED TLVs

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supported LLDP MED TLVs</strong></td>
<td>LLDP-MED TLVs supported on the switch:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>LLDP MED capabilities</strong>—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0—Capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1—Network Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Location Identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—Extended Power via MDI-PSE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4—Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5–15—Reserved</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Network policy</strong>—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Endpoint location</strong>—TLV that advertises the physical location of the endpoint.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Extended power Via MDI</strong>—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

text

show lldp (EX3200 switches)
user@switch> show lldp

```
LLDP                   : Enabled
Advertisement interval : 30 seconds
Transmit delay         : 2 seconds
Hold timer             : 4 seconds
Notification interval  : 0 Second(s)
Config Trap Interval   : 0 seconds
Connection Hold timer  : 300 seconds

LLDP MED               : Disabled
MED fast start count   : 3 Packets

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

text

show lldp (EX4300 switches)
user@switch> show lldp

```
LLDP                   : Enabled
Advertisement interval : 30 seconds
Transmit delay         : 2 seconds
Hold timer             : 120 seconds
Notification interval  : 0 Second(s)
Config Trap Interval   : 0 seconds
Connection Hold timer  : 300 seconds

LLDP MED               : Disabled
MED fast start count   : 3 Packets

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

text

show lldp detail (EX4300 switches)
user@switch> show lldp detail

```
2685
```
LLDP : Enabled
Advertisement interval : 30 seconds
Transmit delay : 2 seconds
Hold timer : 120 seconds
Notification interval : 0 Second(s)
Config Trap Interval : 0 seconds
Connection Hold timer : 300 seconds

LLDP MED : Disabled
MED fast start count : 3 Packets

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Power Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>-</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>100</td>
<td>vlan-100</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>101</td>
<td>vlan-101</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>4000</td>
<td>vlan-4000</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>100</td>
<td>vlan-100</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>101</td>
<td>vlan-101</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>4000</td>
<td>vlan-4000</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>100</td>
<td>vlan-100</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>101</td>
<td>vlan-101</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>4000</td>
<td>vlan-4000</td>
</tr>
</tbody>
</table>

LLDP basic TLVs supported:
Chassis identifier, Port identifier, Port description, System name, System description, System capabilities, Management address.

Supported LLDP 802 TLVs:
MACPHY configuration/status, Power via MDI, Link aggregation, Maximum frame size, Port VLAN tag, Port VLAN name.

Supported LLDP MED TLVs:
LLDP MED capabilities, Network policy, Endpoint location, Extended power Via MDI.

show lldp detail (EX3400 switches with VLAN name TLV)
user@switch> show lldp detail
### LLDP Parameters

- **LLDP**: Enabled
- **Advertisement interval**: 30 seconds
- **Transmit delay**: 2 seconds
- **Hold timer**: 120 seconds
- **Notification interval**: 5 Second(s)
- **Config Trap Interval**: 0 seconds
- **Connection Hold timer**: 300 seconds

### LLDP MED Parameters

- **MED**: Enabled
- **MED fast start count**: 3 Packets

- **Port ID TLV subtype**: locally-assigned
- **Port Description TLV type**: interface-alias (ifAlias)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>-</td>
<td>2</td>
<td>dc-vlan</td>
</tr>
</tbody>
</table>
show lldp local-information

Syntax

```
show lldp local-information
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**

- Configuring LLDP (CLI Procedure) | 654
- Understanding LLDP and LLDP-MED on EX Series Switches | 661
- management-address | 1935
- Understanding LLDP | 653

**List of Sample Output**

*show lldp local-information (EX Series Switch) on page 2690*

**Output Fields**

*Table 90 on page 2689 lists the output fields for the show lldp local-information command. Output fields are listed in the approximate order in which they appear.*
Table 90: show lldp local-information Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Local Information details</td>
<td>Information about the local system (the switch):</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chassis ID</strong>—MAC address associated with the switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>System name</strong>—User-configured name of the switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>System descr</strong>—System description containing information about the switch model and the current software image running on the switch. This information is taken from the software and is not configurable.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Capabilities (such as <strong>bridge</strong> or <strong>router</strong>) that are supported or enabled on the system.</td>
</tr>
<tr>
<td>Management Information</td>
<td>Details of the management information: <strong>Port Name</strong>, <strong>Port Address</strong> (such as 10.204.34.35), <strong>Address Type</strong> (such as ipv4 or ipv6), <strong>Port ID</strong> (SNMP interface index), <strong>Port ID Subtype</strong>, and <strong>Port Subtype</strong>. The <strong>Port Subtype</strong> displays:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ifIndex(2)</strong>—IP address of the switch’s management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a virtual chassis) is used to manage the switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>unknown(1)</strong>—IP management address has been configured with set protocols lldp management-address.</td>
</tr>
<tr>
<td>Interface name</td>
<td>Name of the local interface which is configured for either LLDP or LLDP-MED.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the local interface belongs.</td>
</tr>
<tr>
<td>SNMP Index</td>
<td>SNMP interface index.</td>
</tr>
<tr>
<td>Interface description</td>
<td>User-configured port description.</td>
</tr>
<tr>
<td>Status</td>
<td>Administrative status of the interface: either <strong>up</strong> or <strong>down</strong>.</td>
</tr>
<tr>
<td>Tunneling</td>
<td>Status of tunneling on the interface: either <strong>enabled</strong> or <strong>disabled</strong>.</td>
</tr>
</tbody>
</table>
LLDP Local Information details

Chassis ID   : 00:1d:b5:aa:b9:f0
System name  : switch
System descr : Juniper Networks, Inc. ex8208 , version 10.4I0 [builder] Build 
               date: 2010-11-17 12:38:30 UTC

System Capabilities
   Supported   : Bridge Router
   Enabled     : Bridge Router

Management Information
   Port Name    : -
   Port Address : 10.93.54.6
   Address Type : IPv4
   Port ID      : 34
   Port ID Subtype : local(7)
   Port Subtype : ifIndex(2)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Parent Interface</th>
<th>SNMP Index</th>
<th>Interface description</th>
<th>Status</th>
<th>Tunneling</th>
</tr>
</thead>
<tbody>
<tr>
<td>me0.0</td>
<td>-</td>
<td>34</td>
<td>-</td>
<td>Down</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>769</td>
<td>xe-3/0/0.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>770</td>
<td>xe-3/0/1.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>771</td>
<td>xe-3/0/2.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/3.0</td>
<td>ae31.0</td>
<td>772</td>
<td>xe-3/0/3.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/4.0</td>
<td>ae31.0</td>
<td>577</td>
<td>xe-3/0/4.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/5.0</td>
<td>ae31.0</td>
<td>578</td>
<td>xe-3/0/5.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/6.0</td>
<td>ae31.0</td>
<td>579</td>
<td>xe-3/0/6.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/7.0</td>
<td>ae31.0</td>
<td>581</td>
<td>xe-3/0/7.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
show lldp neighbors

Syntax

```
<show lldp neighbors>
<interface interface-ids>
```

Release Information
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display learned information about Link Layer Discovery Protocol (LLDP) on all neighboring interfaces or on selected interfaces.

Options
none—Display learned LLDP information on all neighboring interfaces and devices.

```
interface interface-ids—(Optional) Display learned LLDP information on the selected interfaces or devices.
```

NOTE: When a port with DCBX enabled begins to exchange type, length, and value (TLV) entries, optional LLDP TLVs on that port are not advertised to neighbors in order to interoperate with a wider variety of converged network adapters (CNAs). As a result, information for those ports will not be listed in the output for this command.

Required Privilege Level
view

RELATED DOCUMENTATION

- Understanding LLDP | 653

List of Sample Output
- show lldp neighbors on page 2694
- show lldp neighbors interface on page 2695

Output Fields
Table 91 on page 2692 lists the output fields for the show lldp neighbors command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Interface</strong></td>
<td>List of local interfaces for which neighbor information is available.</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.</td>
</tr>
<tr>
<td><strong>Chassis ID</strong></td>
<td>List of chassis identifiers for neighbors.</td>
</tr>
<tr>
<td><strong>Port info</strong></td>
<td>List of port information gathered from neighbors. This could be the port identifier or port description.</td>
</tr>
<tr>
<td><strong>System name</strong></td>
<td>List of system names gathered from neighbors.</td>
</tr>
<tr>
<td><strong>LLDP Neighbor Information</strong></td>
<td>Information about both the local system (the switch) and a neighbor system on the interface (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Information</strong></td>
<td>Information about the local system (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>Local interface index (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Time to live</strong></td>
<td>Number of seconds for which this information is valid (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Time mark</strong></td>
<td>Date and timestamp of information (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Interface</strong></td>
<td>Name of the local physical interface (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Port ID</strong></td>
<td>Local interface SNMP index (appears when the interface option is used).</td>
</tr>
<tr>
<td><strong>Ageout Count</strong></td>
<td>Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval has expired (appears when the <code>interface</code> option is used).</td>
</tr>
</tbody>
</table>
Table 91: show lldp neighbors Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Information</td>
<td>Information about a neighbor system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Chassis type</td>
<td>Type of chassis identifier supplied, such as MAC address (appears when the interface option is used).</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis identifier of the chassis type listed (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port type</td>
<td>Type of port identifier supplied, such as locally assigned (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port identifier of the port type listed (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port description</td>
<td>Port description (appears when the interface option is used).</td>
</tr>
<tr>
<td>System name</td>
<td>Name supplied by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>System Description</td>
<td>Description supplied by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>System capabilities</td>
<td>Capabilities (such as Bridge, Router, and Telephone) that are supported or enabled by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Management Info</td>
<td>Details of management information: Type (such as ipv4 or ipv6), Address (such as 10.204.34.35), Port ID, Subtype, Interface Subtype, and organization identifier (OID) (appears when the interface option is used).</td>
</tr>
</tbody>
</table>

The Interface Subtype displays:

- ifIndex(2)—IP address of the neighbor’s management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a virtual chassis) is used to manage the switch.
- unknown(1)—Neighbor’s IP management address has been configured with set protocols lldp management-address.
## Table 91: show lldp neighbors Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Media Info</strong></td>
<td>Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include Media endpoint class (such as Class 3 for communication devices such as IP phones), MED Hardware revision, MED Firmware revision, MED Software revision, MED Serial number, MED Manufacturer name, or MED Model name.</td>
</tr>
<tr>
<td><strong>Organization Info</strong></td>
<td>One or more entries listing remote information by organizationally unique identifier (OUI), Subtype, Index, and Info (appears when the interface option is used).</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>How long the neighbor has been identified (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td><strong>Local Interface</strong></td>
<td>Name of the local physical interface (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td><strong>Chassis ID</strong></td>
<td>Chassis identifier of the chassis type listed (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td><strong>Port description</strong></td>
<td>Port description (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td><strong>System name</strong></td>
<td>NetBIOS name of the host (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
</tbody>
</table>

### Sample Output

```
show lldp neighbors
user@switch> show lldp neighbors
```

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>Parent Interface</th>
<th>Chassis Id</th>
<th>Port info</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2694</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show lldp neighbors interface
duser@switch> show lldp neighbors interface ge-0/0/2

LLDP Neighbor Information:
Local Information:
Local Interface : ge-0/0/2.0
Parent Interface : -
Local Port ID : 507
Ageout Count : 0

Neighbour Information:
Chassis type : Mac address
Chassis ID : 00:1f:12:38:7f:c0
Port type : Locally assigned
Port ID : 507
Port description : ge-0/0/2.0
System name : bng-148p5-dev

System Description : Juniper Networks, Inc. ex4200-48p, version 10.4I0 Build date: 2010-11-30 09:32:17 UTC

System capabilities
Supported : Bridge Router
Enabled : Bridge Router

Management Info
Type : IPv4
Address : 10.204.96.235
Port ID : 34
Subtype : 1
Interface Subtype : ifIndex(2)
OID : 1.3.6.1.2.1.31.1.1.1.1.34

Media endpoint class: Network Connectivity

Organization Info
OUI : 0.12.f
Subtype : 1
Index : 1
Info : 22A8360000

Organization Info
OUI : 0.12.f
Subtype : 2
Index : 2
Info : 030100
show lldp neighbors

Syntax

```
show lldp neighbors
<interface interface>
```

Release Information

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

Description

Display the information about neighboring devices learned by the switch by using the Link Layer Discovery Protocol (LLDP).

NOTE: The Chassis ID TLV has a subtype for Network Address Family. The supported network address families are IPv4 and IPv6. LLDP frames are validated only if the Network Address subtype of the Chassis ID TLV has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the `show lldp neighbors` command, but is not assigned to the VLAN.

Options

```
interface interface—(Optional) Display LLDP neighbor information for a selected interface.
```

Required Privilege Level

view

RELATED DOCUMENTATION

| Configuring LLDP (CLI Procedure) | 654 |
| Understanding LLDP and LLDP-MED on EX Series Switches | 661 |

List of Sample Output

- `show lldp neighbors` on page 2700
- `show lldp neighbors interface ge-0/0/8` on page 2701
- `show lldp neighbors interface ge-0/0/0.0 (for a VoIP Avaya Telephone with LLDP-MED Support)` on page 2702
- `show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)` on page 2704

Output Fields
Table 91 on page 2692 lists the output fields for the `show lldp neighbors` command. Output fields are listed in the approximate order in which they appear.

**Table 92: show lldp neighbors Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Interface</strong></td>
<td>List of local interfaces for which neighbor information is available.</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.</td>
</tr>
<tr>
<td><strong>Chassis ID</strong></td>
<td>List of chassis identifiers for neighbors.</td>
</tr>
<tr>
<td><strong>Port info</strong></td>
<td>This field displays the port information received from neighbors.</td>
</tr>
<tr>
<td><strong>System name</strong></td>
<td>List of system names gathered from neighbors. Includes the host name and the domain name.</td>
</tr>
<tr>
<td><strong>LLDP Neighbor Information</strong></td>
<td>Information about both the local system (the switch) and a neighbor system on the interface (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Information</strong></td>
<td>Information about the local system (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>Local interface index (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Time to live</strong></td>
<td>Number of seconds for which this information is valid (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Time mark</strong></td>
<td>Date and timestamp of information (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Interface</strong></td>
<td>Name of the local physical interface (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Parent Interface</strong></td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the <code>interface</code> option is used).</td>
</tr>
<tr>
<td><strong>Local Port ID</strong></td>
<td>Local interface SNMP index (appears when the interface option is used).</td>
</tr>
<tr>
<td><strong>Ageout Count</strong></td>
<td>Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval expired (appears when the interface option is used).</td>
</tr>
</tbody>
</table>
Table 92: show lldp neighbors Output Fields  *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Information</td>
<td>Information about a neighbor system on the interface (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Chassis type</td>
<td>Type of chassis identifier supplied, such as <em>Mac address</em> (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis identifier of the chassis type listed (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Port type</td>
<td>Type of port identifier supplied, such as <em>Locally assigned</em> (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port identifier of the port type listed (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Port description</td>
<td>The port description field uses the configured port description, the port name or the SNMP ifIndex (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>System name</td>
<td>Name supplied by the system on the interface (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>System Description</td>
<td>Description supplied by the system on the interface (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>System capabilities</td>
<td>Capabilities (such as <em>Bridge</em>, <em>Bridge Router</em>, and <em>Bridge Telephone</em>) that are supported or enabled by the system on the interface (appears when the <em>interface</em> option is used).</td>
</tr>
<tr>
<td>Management Info</td>
<td>Details of management information: <em>Type</em> (such as <em>IPv4</em> or <em>IPv6</em>), <em>Address</em> (such as <em>10.204.34.35</em>), <em>Port ID</em>, <em>Subtype</em>, <em>Interface Subtype</em>, and organization identifier (<em>OID</em>) (appears when the <em>interface</em> option is used).</td>
</tr>
</tbody>
</table>

The *Interface Subtype* displays:

- *ifIndex(2)*—IP address of the neighbor’s management Ethernet interface (*me0*) or virtual management Ethernet (*VME*) interface address (for a Virtual Chassis) is used to manage the switch.
- *unknown(1)*—Neighbor’s IP management address has been configured with set *protocols lldp management-address*.  

2699
Table 92: show lldp neighbors Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Info</td>
<td>Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: Media endpoint class (such as Class 3 for communication devices such as IP phones), MED Hardware revision, MED Firmware revision, MED Software revision, MED Serial number, MED Manufacturer name, MED Model name.</td>
</tr>
<tr>
<td>Organization Info</td>
<td>One or more entries (indexed by the Index element) listing more remote interface information by organizationally unique identifier (OUI), Subtype, and Info (appears when the interface option is used).</td>
</tr>
<tr>
<td>Age</td>
<td>How long the neighbor has been identified (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the local physical interface (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis identifier of the chassis type listed (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
</tbody>
</table>

Sample Output

```
show lldp neighbors

user@switch> show lldp neighbors

Local Interface   Parent Interface   Chassis Id          Port info    System Name
xe-3/0/4.0       ae31.0             b0:c6:9a:63:80:40   xe-0/0/0.0   host.jnpr.net
xe-3/0/5.0       ae31.0             b0:c6:9a:63:80:40   xe-0/0/1.0   host.jnpr.net
xe-3/0/6.0       ae31.0             b0:c6:9a:63:80:40   xe-0/0/2.0   host.jnpr.net
xe-3/0/7.0       ae31.0             b0:c6:9a:63:80:40   xe-0/0/3.0   host.jnpr.net
xe-3/0/0.0       ae31.0             b0:c6:9a:63:80:40   xe-0/1/0.0   host.jnpr.net
xe-3/0/1.0       ae31.0             b0:c6:9a:63:80:40   xe-0/1/1.0   host.jnpr.net
```
show lldp neighbors interface ge-0/0/8

user@switch> show lldp neighbors interface ge-0/0/8

LLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 120 Time mark: Thu Nov 26 06:41:24 2015 Age: 1 secs
Local Interface : ge-0/0/8
Parent Interface : -
Local Port ID : 518
Ageout Count : 0

Neighbour Information:
Chassis type : Mac address
Chassis ID : 88:e0:f3:1f:14:e0
Port type : Locally assigned
Port ID : 880
Port description : ge-0/0/8
System name : bng-nw6moj.juniper.net

System Description : Juniper Networks, Inc. ex4300-24p Ethernet Switch, kernel JUNOS 14.1I20151125_0548_rajjs, Build date: 2015-11-25 06:06:58 UTC Copyright (c) 1996-2015 Juniper Networks, Inc.

System capabilities
   Supported: Bridge Router
   Enabled: Bridge Router

Management address
   Address Type: IPv4(1)
   Address: 10.204.39.232
   Interface Number: 33
   Interface Subtype: ifIndex(2)
   OID: 1.3.6.1.2.1.31.1.1.1.1.33.

Media endpoint class: Network Connectivity

Organization Info
   OUI: IEEE 802.3 Private (0x00120f)
   Subtype: MAC/PHY Configuration/Status (1)
   Info: Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation
Capability (0x1), MAU Type (0x0)
Index : 1

Organization Info
OUI : IEEE 802.3 Private (0x00120f)
Subtype : MDI Power (2)
Info : MDI Power Support [PSE bit set, supported, disabled, CONTROL bit not set (0x3)], MDI Power Pair [signal], MDI Power Class [Unknown (7)]
Index : 2

Organization Info
OUI : IEEE 802.3 Private (0x00120f)
Subtype : Link Aggregation (3)
Info : Aggregation Status [supported, disabled (0x1)], Aggregation Port ID (0)
Index : 3

Organization Info
OUI : IEEE 802.3 Private (0x00120f)
Subtype : Maximum Frame Size (4)
Info : MTU Size (1514)
Index : 4

Organization Info
OUI : Juniper Specific (0x009069)
Subtype : Chassis Serial Type (1)
Info : Juniper Slot Serial [MS3112240009]
Index : 5

show lldp neighbors interface ge-0/0/0.0 (for a VoIP Avaya Telephone with LLDP-MED Support)
user@switch> show lldp neighbors interface ge-0/0/0.0

LLDP Neighbor Information:
Local Information:
Index: 20 Time to live: 120 Time mark: Thu Apr 15 22:26:22 2010 Age: 16 secs
Local Interface : ge-0/0/0.0
Parent Interface : -
Local Port ID : 517
Ageout Count : 0

Neighbour Information:
Chassis type : Network address
Chassis ID         : 0.0.0.0  
Port type          : Mac address  
Port ID            : 00:04:0d:fc:55:48  
System name        : AVAFC5548.juniper.net

System capabilities
   Supported : Bridge Telephone  
   Enabled   : Bridge

Management Info
   Type       : IPv4  
   Address    : 0.0.0.0  
   Port ID    : 1  
   Subtype    : 1  
   Interface Subtype : ifIndex(2)  
   OID        : 1.3.6.1.2.1.31.1.1.1.1.1
Media endpoint class: Class III Device

MED Hardware revision : 4610D01A  
MED Firmware revision : b10d01b2_9.bin  
MED Software revision : a10d01b2_9.bin  
MED Serial number     : 07N510103424  
MED Manufacturer name : Avaya  
MED Model name        : 4610

Organization Info
   OUI      : IEEE 802.3 Private (0x00120f)  
   Subtype  : MAC/PHY Configuration/Status (1)  
   Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x1d00), MAU Type (0x0)  
   Index    : 1

Organization Info
   OUI      : IEEE 802.3 Private (0x00120f)  
   Subtype  : MDI Power (2)  
   Info     : MDI Power Support [PSE bit set, supported, disabled, CONTROL bit not set (0x3)], MDI Power Pair [signal], MDI Power Class [Unknown (7)]  
   Index    : 2

Organization Info
   OUI      : IEEE 802.3 Private (0x00120f)  
   Subtype  : Link Aggregation (3)  
   Info     : Aggregation Status [supported, disabled (0x1)], Aggregation Port ID (0)
show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)

user@switch> show lldp neighbors interface ge-0/0/5

Age: 299999 secs
Local Interface : ge-0/0/5.0
Parent Interface : -
Chassis ID : 00:10:94:00:00:02
Port description : 192.0.2.1
System name : host.juniper.net
show lldp remote-global-statistics

Syntax

```
show lldp remote-global-statistics
```

Release Information
Command introduced in Junos OS Release 10.0 for EX Series switches.

Description
Display remote Link Layer Discovery Protocol (LLDP) global statistics.

Options
This command has no options.

Required Privilege Level
view

RELATED DOCUMENTATION

- Configuring LLDP (CLI Procedure) | 654
- Understanding LLDP and LLDP-MED on EX Series Switches | 661

List of Sample Output
show lldp remote-global-statistics on page 2706

Output Fields
Table 93 on page 2705 describes the output fields for the `show lldp remote-global-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 93: show lldp remote-global-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Remote Database Table Counters</td>
<td>Information about remote database table counters.</td>
</tr>
<tr>
<td>LastChangeTime</td>
<td>Time elapsed between LLDP agent startup and the last change to the remote database table information.</td>
</tr>
<tr>
<td>Inserts</td>
<td>Number of insertions made in the remote database table.</td>
</tr>
</tbody>
</table>
Table 93: show lldp remote-global-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletes</td>
<td>Number of deletions made in the remote database table.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of LLDP frames dropped from the remote database table because of errors.</td>
</tr>
<tr>
<td>Ageouts</td>
<td>Number of remote database table entries that have aged out of the table.</td>
</tr>
</tbody>
</table>

Sample Output

show lldp remote-global-statistics

user@host> show lldp remote-global-statistics

user@host> show lldp remote-global-statistics

LLDP Remote Database Table Counters

<table>
<thead>
<tr>
<th>LastchangeTime</th>
<th>Inserts</th>
<th>Deletes</th>
<th>Drops</th>
<th>Ageouts</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:76 (76 sec)</td>
<td>192</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show lldp statistics

Syntax

show lldp statistics
<interface interface-ids>

Release Information
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description
Display LLDP statistics on all or selected interfaces.

Options

none—Display LLDP statistics on all interfaces and devices.

interface interface-ids—(Optional) Display LLDP statistics on the selected devices.

Required Privilege Level
view

RELATED DOCUMENTATION

Understanding LLDP | 653

List of Sample Output

show lldp statistics on page 2708

Output Fields

Table 94 on page 2707 lists the output fields for the show lldp statistics command. Output fields are listed in the approximate order in which they appear.

Table 94: show lldp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of an interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Received</td>
<td>Total number of LLDP frames received on an interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unknown-TLVs</td>
<td>Number of unrecognized LLDP TLVs received on an interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 94: show lldp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>With Errors</td>
<td>Number of LLDP frames received that contain errors.</td>
<td>All levels</td>
</tr>
<tr>
<td>Discarded TLVs</td>
<td>Number of LLDP TLVs received and then discarded on an interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Total number of LLDP frames transmitted on an interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Untransmitted</td>
<td>Total number of LLDP frames not transmitted on an interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show lldp statistics

```
user@switch> show lldp statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
<th>Discarded TLVs</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>me0.0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8003</td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>8002</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8003</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>8002</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8003</td>
</tr>
</tbody>
</table>
```
# show lldp statistics

## Syntax

```
show lldp statistics
<interface interface>
```

## Release Information

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

## Description

Display LLDP statistics for all interfaces or for the specified interface.

## Options

- **none**—Display LLDP statistics for all interfaces.
- **interface interface**—(Optional) Display LLDP statistics for the specified interface.

## Required Privilege Level

```
view
```

## RELATED DOCUMENTATION

- [Configuring LLDP (CLI Procedure)](#) | 654
- [Understanding LLDP and LLDP-MED on EX Series Switches](#) | 661

## List of Sample Output

- show lldp statistics on page 2710
- show lldp statistics interface xe-3/0/0.0 on page 2711

## Output Fields

Table 94 on page 2707 lists the output fields for the `show lldp statistics` command. Output fields are listed in the approximate order in which they appear.

### Table 95: show lldp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
</tbody>
</table>
Table 95: show lldp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Parent Interface | Name of the aggregated Ethernet interface, if any, to which the interface belongs.  

**NOTE:** Because LLDP packets are transmitted and received on member interfaces only, statistics are available only for the member interfaces, not for the aggregated interface.  

<table>
<thead>
<tr>
<th>Received</th>
<th>Total number of LLDP frames received on an interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown TLVs</td>
<td>Number of unrecognized LLDP TLVs received on an interface.</td>
</tr>
<tr>
<td>With Errors</td>
<td>Number of invalid LLDP TLVs received on an interface.</td>
</tr>
<tr>
<td>Discarded</td>
<td>Number of LLDP TLVs received and then discarded on an interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Total number of LLDP frames that were transmitted on an interface.</td>
</tr>
<tr>
<td>Untransmitted</td>
<td>Total number of LLDP frames that were untransmitted on an interface.</td>
</tr>
</tbody>
</table>

Sample Output

```
show lldp statistics

user@switch> show lldp statistics
```

```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Received</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>1564</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>1564</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>1565</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/3.0</td>
<td>ae31.0</td>
<td>1566</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/4.0</td>
<td>ae31.0</td>
<td>1598</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/5.0</td>
<td>ae31.0</td>
<td>1598</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/6.0</td>
<td>ae31.0</td>
<td>1596</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/7.0</td>
<td>ae31.0</td>
<td>1597</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-5/0/6.0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-5/0/7.0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show lldp statistics interface xe-3/0/0.0

user@switch> show lldp statistics interface xe-3/0/0.0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Received</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>1566</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Discarded TLVs  Transmitted  Untransmitted
0                3046          1
**show network-access aaa statistics accounting**

**Syntax**

```
show network-access aaa statistics accounting;
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

**Description**
Display authentication, authorization, and accounting (AAA) accounting statistics.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**
- accounting-server | 1466
- accounting-stop-on-access-deny | 1468
- Configuring 802.1X RADIUS Accounting (CLI Procedure) | 438

**List of Sample Output**
show network-access aaa statistics accounting on page 2713

**Output Fields**
Table 96 on page 2712 lists the output fields for the `show network-access aaa statistics accounting` command. Output fields are listed in the approximate order in which they appear.

**Table 96: show network-access aaa statistics accounting Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of accounting-request packets sent from a switch to a RADIUS accounting server.</td>
</tr>
<tr>
<td>Accounting Response failures</td>
<td>The number of accounting-response failure packets sent from the RADIUS accounting server to the switch.</td>
</tr>
<tr>
<td>Accounting Response Success</td>
<td>The number of accounting-response success packets sent from the RADIUS accounting server to the switch.</td>
</tr>
</tbody>
</table>
Table 96: show network-access aaa statistics accounting Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests timedout</td>
<td>The number of requests-timedout packets sent from the RADIUS accounting server to the switch.</td>
</tr>
</tbody>
</table>

Sample Output

```
show network-access aaa statistics accounting
user@switch> show network-access aaa statistics accounting

Accounting module statistics
    Requests received: 1
    Accounting Response failures: 0
    Accounting Response Success: 1
    Requests timedout: 0
```
**show network-access aaa statistics authentication**

**Syntax**

```
show network-access aaa statistics authentication
```

**Release Information**

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

**Description**

Display authentication, authorization, and accounting (AAA) authentication statistics.

**Required Privilege Level**

`view`

**RELATED DOCUMENTATION**

- [authentication-server | 1527](#)
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch | 400

**List of Sample Output**

- show network-access aaa statistics authentication on page 2715
- show network-access aaa statistics authentication (in QFX Series Switches) on page 2715

**Output Fields**

Table 97 on page 2714 lists the output fields for the `show network-access aaa statistics authentication` command. Output fields are listed in the approximate order in which they appear.

**Table 97: show network-access aaa statistics authentication Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of authentication requests received by the switch.</td>
</tr>
<tr>
<td>Accepts</td>
<td>The number of authentication accepts received by the RADIUS server.</td>
</tr>
<tr>
<td>Rejects</td>
<td>The number authentication rejects sent by the RADIUS server.</td>
</tr>
<tr>
<td>Challenges</td>
<td>The number of authentication challenges sent by the RADIUS server.</td>
</tr>
</tbody>
</table>
Sample Output

show network-access aaa statistics authentication

user@switch> show network-access aaa statistics authentication

Authentication module statistics
  Requests received: 2
  Accepts: 1
  Rejects: 0
  Challenges: 1

show network-access aaa statistics authentication (in QFX Series Switches)

user@switch> show network-access aaa statistics authentication

Authentication module statistics
  Requests received: 2
  Accepts: 1
  Rejects: 0
  Challenges: 1
show network-access aaa statistics dynamic-requests

Syntax

```
show network-access aaa statistics dynamic-requests;
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

Description
Display authentication, authorization, and accounting (AAA) authentication statistics for disconnects.

Required Privilege Level
view

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>authentication-server</th>
<th>1527</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch</td>
<td>400</td>
</tr>
</tbody>
</table>

List of Sample Output

show network-access aaa statistics authentication on page 2717

Output Fields

Table 98 on page 2716 lists the output fields for the `show network-access aaa statistics dynamic-requests` command. Output fields are listed in the approximate order in which they appear.

Table 98: show network-access aaa statistics dynamic-requests Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of dynamic requests received by the RADIUS server.</td>
</tr>
<tr>
<td>Processed successfully</td>
<td>The number of dynamic requests successfully processed by the RADIUS server.</td>
</tr>
<tr>
<td>Errors during processing</td>
<td>The number of errors that occurred while the RADIUS server was processing the dynamic request.</td>
</tr>
<tr>
<td>Silently dropped</td>
<td>The number of silently dropped requests.</td>
</tr>
</tbody>
</table>
Sample Output

```
show network-access aaa statistics authentication
user@switch> show network-access aaa statistics dynamic-requests

Dynamic-requests module statistics
  Requests received: 0
  Processed successfully: 0
  Errors during processing: 0
  Silently dropped: 0
```
show network-access radsec local-certificate

Syntax

show network-access radsec local-certificate
  <state>
  <statistics [brief | detail | extensive]>
  <certificate-name>

Release Information
Command introduced in Junos OS Release 19.1R1.

Description
Display the state and statistics of local certificate acquisition. RADSEC uses local certificates dynamically acquired from the public key infrastructure to establish a TLS connection.

If a certificate is not available, or if it was revoked, the RADSEC client will try to retrieve it every 300 seconds. Response timeout is 10 seconds, and failures are retried in 10 seconds.

Options
state—Display the state of acquisition for the local certificate.

statistics—Display acquisition statistics for the local certificate.

brief | detail | extensive—(Optional) Display the specified level of output.

certificate-name—(Optional) Display detailed information about the specified certificate.

Required Privilege Level
table

RELATED DOCUMENTATION

RADIUS over TLS (RADSEC) | 259

List of Sample Output
show network-access radsec local-certificate state on page 2719
show network-access radsec local-certificate statistics on page 2719
show network-access radsec local-certificate statistics detail on page 2720

Output Fields
Table 99 on page 2719 lists the output fields for the show network-access local-certificate command. Output fields are listed in the approximate order in which they appear.
Table 99: show network-access radsec local-certificate Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local certificate state</td>
<td>State of acquisition for the local certificate.</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>• active—Local certificate is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• waiting—Waiting to acquire local certificate.</td>
<td></td>
</tr>
<tr>
<td>Local certificate general</td>
<td>Statistics for RADSEC local certificate acquisition.</td>
<td>all</td>
</tr>
<tr>
<td>counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: Default output level will list only non-zero counters. Use detail or extensive to view all counters.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

**show network-access radsec local-certificate state**

```
user@host> show network-access radsec local-certificate state

Local certificate state:
cert-2                        active
cert-4                        waiting
qqq                            waiting
```

**show network-access radsec local-certificate statistics**

```
user@host> show network-access radsec local-certificate statistics

Local certificate general counters:
total-requests                36
```
### Sample Output

```
show network-access radsec local-certificate statistics detail

user@host> show network-access radsec local-certificate statistics detail

Local certificate general counters:
  - total-requests: 36
  - failed-requests: 0
  - total-responses: 0
  - configured-responses: 0
```
show network-access radsec statistics

Syntax

```
show network-access radsec statistics
  <[brief | detail | extensive]>
  <destination destination-id>
```

Release Information

Command introduced in Junos OS Release 19.1R1.

Description

Display the connection statistics for the RADSEC destinations.

Options

- `brief | detail | extensive`—(Optional) Display the specified level of output. The default is `brief`, which will list only non-zero counters.

- `destination destination-id`—(Optional) Display detailed information about the request specified by this RADSEC destination.

Required Privilege Level

`view`

RELATED DOCUMENTATION

- `RADIUS over TLS (RADSEC) | 259`

List of Sample Output

- `show network-access radsec statistics on page 2722`
- `show network-access radsec statistics detail on page 2722`

Output Fields

`Table 100 on page 2722` lists the output fields for the `show network-access statistics` command. Output fields are listed in the approximate order in which they appear.
Table 100: show network-access radsec statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radsec general counters</td>
<td>Statistics for RADSEC syslog event counters.</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Default output level will list only non-zero counters. Use detail or extensive to show all counters.</td>
</tr>
<tr>
<td>Destination</td>
<td>ID number of the RADSEC destination.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

show network-access radsec statistics

user@host> show network-access radsec statistics

Radsec general counters:

  destination             895
  start-events             1
  clear-events             1
  timeout-events           1
  loc-cert-acq-events      1
  connected-events         1
  ssl-ready-events         1

Sample Output

show network-access radsec statistics detail

user@host> show network-access radsec statistics detail

Radsec general counters:

  destination             895
  start-events             1
  clear-events             1
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>force-disconnect-events</td>
<td>0</td>
</tr>
<tr>
<td>timeout-events</td>
<td>1</td>
</tr>
<tr>
<td>loc-cert-acq-events</td>
<td>1</td>
</tr>
<tr>
<td>loc-cert-lost-events</td>
<td>0</td>
</tr>
<tr>
<td>connected-events</td>
<td>1</td>
</tr>
<tr>
<td>conn-failed-events</td>
<td>0</td>
</tr>
<tr>
<td>ssl-disconnected-events</td>
<td>0</td>
</tr>
<tr>
<td>ssl-ready-events</td>
<td>1</td>
</tr>
<tr>
<td>in-auth-reqs</td>
<td>0</td>
</tr>
<tr>
<td>in-acct-reqs</td>
<td>0</td>
</tr>
<tr>
<td>in-dyn-req-resps</td>
<td>0</td>
</tr>
<tr>
<td>tx-auth-reqs</td>
<td>0</td>
</tr>
<tr>
<td>tx-acct-reqs</td>
<td>0</td>
</tr>
<tr>
<td>tx-wd-reqs</td>
<td>9</td>
</tr>
<tr>
<td>tx-late-auth-reqs</td>
<td>0</td>
</tr>
<tr>
<td>tx-late-acct-reqs</td>
<td>0</td>
</tr>
<tr>
<td>tx-dyn-req-resps</td>
<td>0</td>
</tr>
<tr>
<td>rx-auth-resps</td>
<td>0</td>
</tr>
<tr>
<td>rx-acct-resps</td>
<td>0</td>
</tr>
<tr>
<td>rx-dyn-reqs</td>
<td>0</td>
</tr>
<tr>
<td>rx-dyn-req-naks</td>
<td>0</td>
</tr>
<tr>
<td>rx-dyn-req-drops</td>
<td>0</td>
</tr>
<tr>
<td>rx-wd-resps</td>
<td>9</td>
</tr>
<tr>
<td>rx-resps</td>
<td>0</td>
</tr>
<tr>
<td>rx-late-resps</td>
<td>0</td>
</tr>
<tr>
<td>rx-other-drops</td>
<td>0</td>
</tr>
<tr>
<td>resp-disconnect-drops</td>
<td>0</td>
</tr>
<tr>
<td>id-disconnect-drops</td>
<td>0</td>
</tr>
<tr>
<td>id-timeout-drops</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-no-acct-supports</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-dest-downs</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-overflows</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-disconnects</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-bad-responses</td>
<td>0</td>
</tr>
<tr>
<td>tx-req-id-reuse-timeouts</td>
<td>0</td>
</tr>
<tr>
<td>tx-resp-dest-downs</td>
<td>0</td>
</tr>
<tr>
<td>tx-wd-reqs</td>
<td>9</td>
</tr>
<tr>
<td>rx-wd-resps</td>
<td>9</td>
</tr>
</tbody>
</table>
show network-access radsec state

Syntax

    show network-access radsec state
    <destination destination-id>

Release Information
Command introduced in Junos OS Release 19.1R1.

Description
Display the connection state of RADSEC destinations.

Options
destination destination-id—(Optional) Display detailed information about the request specified by this RADSEC destination.

Required Privilege Level
view

RELATED DOCUMENTATION

    RADIUS over TLS (RADSEC) | 259

List of Sample Output
show network-access radsec state on page 2725

Output Fields
Table 101 on page 2724 lists the output fields for the show network-access state command. Output fields are listed in the approximate order in which they appear.

Table 101: show network-access radsec state Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radsec state</td>
<td>State information for the RADSEC destination.</td>
<td>all</td>
</tr>
</tbody>
</table>
Table 101: show network-access radsec state Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>State of the RADSEC connection.</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>• connecting—Establishing TCP connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ssl-handshake—SSL negotiation in progress.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• open—RADSEC session is established for exchange of RADIUS messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pause—Pause for restart of connection process. The length of the pause is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>determined by the reason for restarting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• local-cert-wait—Connection initiated but waiting for local certificate to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>complete negotiation.</td>
<td></td>
</tr>
<tr>
<td>secs-in-state</td>
<td>Length of time in seconds of the current state.</td>
<td>all</td>
</tr>
<tr>
<td>remaining-secs</td>
<td>Length of time in seconds remaining for the current state.</td>
<td>all</td>
</tr>
<tr>
<td>pause-reason</td>
<td>The reason for restarting the connection, which triggers the pause state.</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>The pause reason determines the length of the pause until reattemping the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>connection.</td>
<td></td>
</tr>
<tr>
<td>acct-support</td>
<td>Shows whether the remote server supports accounting.</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>• Y—Remote server supports accounting. This is the default value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• N—If the client receives a NAK response to an accounting request, all</td>
<td></td>
</tr>
<tr>
<td></td>
<td>accounting requests will be dropped.</td>
<td></td>
</tr>
<tr>
<td>remote-failures</td>
<td>Number of consecutive failures on the remote side.</td>
<td>all</td>
</tr>
<tr>
<td>tx-requests</td>
<td>Number of RADIUS request messages transmitted.</td>
<td>all</td>
</tr>
<tr>
<td>tx-responses</td>
<td>Number of RADIUS response messages transmitted.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

```
show network-access radsec state
user@host> show network-access radsec state

Radsec state:
        destination                      895
```
<table>
<thead>
<tr>
<th>state</th>
<th>open</th>
</tr>
</thead>
<tbody>
<tr>
<td>secs-in-state</td>
<td>66</td>
</tr>
<tr>
<td>remaining-secs</td>
<td>4294967295</td>
</tr>
<tr>
<td>pause-reason</td>
<td>none</td>
</tr>
<tr>
<td>acct-support</td>
<td>Y</td>
</tr>
<tr>
<td>remote-failures</td>
<td>0</td>
</tr>
<tr>
<td>tx-requests</td>
<td>0</td>
</tr>
<tr>
<td>tx-responses</td>
<td>0</td>
</tr>
</tbody>
</table>
show route extensive

List of Syntax
Syntax on page 2727
Syntax (EX Series Switches) on page 2727

Syntax

```
show route extensive
  <destination-prefix>
  <logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route extensive
  <destination-prefix>
```

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

Description
Display extensive information about the active entries in the routing tables.

Options
none—Display all active entries in the routing table.

destination-prefix—(Optional) Display active entries for the specified address or range of addresses.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level
view

List of Sample Output
show route extensive on page 2736
show route extensive (Access Route) on page 2746
show route extensive (BGP PIC Edge) on page 2747
show route extensive (FRR and LFA) on page 2748
show route extensive (IS-IS) on page 2749
show route extensive (Route Reflector) on page 2749
show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2750
Output Fields

Table 102 on page 2728 describes the output fields for the `show route extensive` command. Output fields are listed in the approximate order in which they appear.

### Table 102: show route extensive Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
</tbody>
</table>
| number routes      | Number of routes in the routing table and total number of routes in the following states:  
  - active (routes that are active).  
  - holdown (routes that are in the pending state before being declared inactive).  
  - hidden (routes that are not used because of a routing policy).                                                                                                                                                                                                                     |
| route-destination  | Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:  
  - MPLS-label (for example, 80001).  
  - interface-name (for example, ge-1/0/2).  
  - neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local/96).  
  - neighbor-address—Address of the neighbor.  
  - control-word-status—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord.  
  - encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.  
  - vc-id—Virtual circuit identifier.  
  - source—Source of the advertisement: **Local** or **Remote**.                                                                                                                                                                                                                   |
| TSI                | Protocol header information.                                                                                                                                                                                                                                                                                                                          |
### Table 102: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| label stacking    | (Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels.  
  - **S=0 route** indicates that a packet with an incoming label stack depth of two or more exits this router with one fewer label (the label-popping operation is performed).  
  - If there is no **S=** information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed). |
| [protocol, preference] | Protocol from which the route was learned and the preference value for the route.  
  - +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.  
  - -—A hyphen indicates the last active route.  
  - *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.  
  In every routing metric except for the BGP **LocalPref** attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1’s complement of the **LocalPref** value in the **Preference2** field. For example, if the **LocalPref** value for Route 1 is 100, the **Preference2** value is -101. If the **LocalPref** value for Route 2 is 155, the **Preference2** value is -156. Route 2 is preferred because it has a higher **LocalPref** value and a lower **Preference2** value. |
| Level             | (IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs. |
| Route Distinguisher | IP subnet augmented with a 64-bit prefix. |
| PMSI              | Provider multicast service interface (MVPN routing table). |
| Next-hop type     | Type of next hop. For a description of possible values for this field, see the Output Field table in the `show route detail` command. |
| Next-hop reference count | Number of references made to the next hop. |
Table 102: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood nexthop branches exceed maximum message</td>
<td>Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.</td>
</tr>
<tr>
<td>Source</td>
<td>IP address of the route source.</td>
</tr>
<tr>
<td>Next hop</td>
<td>Network layer address of the directly reachable neighboring system.</td>
</tr>
</tbody>
</table>
| via                                            | Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word Selected. This field can also contain the following information:  
  • Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.  
  • Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.                                                                                                                                 |
<p>| Label-switched-path lsp-path-name              | Name of the LSP used to reach the next hop.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Label operation                                | MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).                                                                                                                                                                                                                                                                                       |
| Offset                                         | Whether the metric has been increased or decreased by an offset value.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Interface                                      | (Local only) Local interface name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Protocol next hop                              | Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.                                                                                                                                                                                                                                                                                                                                                      |
| label-operation                                | MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).                                                                                                                                                                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Indirect next hops** | When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved.  
When BGP PIC Edge is enabled, the output lines that contain **Indirect next hop: weight** follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values:  
- 0x1 indicates active next hops.  
- 0x4000 indicates passive next hops. |
| **State**      | State of the route (a route can be in more than one state). See the Output Field table in the `show route detail` command.                                                                                           |
| **Session ID** | The BFD session ID number that represents the protection using MPLS fast reroute (FRR) and loop-free alternate (LFA).                                                                                            |
| **Weight**     | Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown.  
For sample output, see `show route table`.                                                                                                  |
### Table 102: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactive reason</strong></td>
<td>If the route is inactive, the reason for its current state is indicated. Typical reasons include:</td>
</tr>
<tr>
<td>• Active preferred</td>
<td>Currently active route was selected over this route.</td>
</tr>
<tr>
<td>• Always compare MED</td>
<td>Path with a lower multiple exit discriminator (MED) is available.</td>
</tr>
<tr>
<td>• AS path</td>
<td>Shorter AS path is available.</td>
</tr>
<tr>
<td>• Cisco Non-deterministic MED selection</td>
<td>Cisco nondeterministic MED is enabled and a path with a lower MED is available.</td>
</tr>
<tr>
<td>• Cluster list length</td>
<td>Path with a shorter cluster list length is available.</td>
</tr>
<tr>
<td>• Forwarding use only</td>
<td>Path is only available for forwarding purposes.</td>
</tr>
<tr>
<td>• IGP metric</td>
<td>Path through the next hop with a lower IGP metric is available.</td>
</tr>
<tr>
<td>• IGP metric type</td>
<td>Path with a lower OSPF link-state advertisement type is available.</td>
</tr>
<tr>
<td>• Interior &gt; Exterior &gt; Exterior via Interior</td>
<td>Direct, static, IGP, or EBGP path is available.</td>
</tr>
<tr>
<td>• Local preference</td>
<td>Path with a higher local preference value is available.</td>
</tr>
<tr>
<td>• Next hop address</td>
<td>Path with a lower metric next hop is available.</td>
</tr>
<tr>
<td>• No difference</td>
<td>Path from a neighbor with a lower IP address is available.</td>
</tr>
<tr>
<td>• Not Best in its group</td>
<td>Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process. When this reason is displayed, an additional reason is provided (typically one of the other reasons listed).</td>
</tr>
<tr>
<td>• Number of gateways</td>
<td>Path with a higher number of next hops is available.</td>
</tr>
<tr>
<td>• Origin</td>
<td>Path with a lower origin code is available.</td>
</tr>
<tr>
<td>• OSPF version</td>
<td>Path does not support the indicated OSPF version.</td>
</tr>
<tr>
<td>• RIB preference</td>
<td>Route from a higher-numbered routing table is available.</td>
</tr>
<tr>
<td>• Route distinguisher</td>
<td>64-bit prefix added to IP subnets to make them unique.</td>
</tr>
<tr>
<td>• Route metric or MED comparison</td>
<td>Route with a lower metric or MED is available.</td>
</tr>
<tr>
<td>• Route preference</td>
<td>Route with a lower preference value is available.</td>
</tr>
<tr>
<td>• Router ID</td>
<td>Path through a neighbor with a lower ID is available.</td>
</tr>
<tr>
<td>• Unusable path</td>
<td>Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved.</td>
</tr>
<tr>
<td>• Update source</td>
<td>Last tiebreaker is the lowest IP address value.</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>Autonomous system (AS) number of the local routing device.</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td><strong>AIGP</strong></td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.</td>
</tr>
<tr>
<td>MED-plus-IGP</td>
<td>Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.</td>
</tr>
<tr>
<td>TTL-Action</td>
<td>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances.</td>
</tr>
<tr>
<td></td>
<td>For sample output, see <code>show route table</code>.</td>
</tr>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>List of protocols that are consumers of the route. Using the following output as an example, <code>Announcement bits (3): 0-KRT 5-Resolve tree 2 8-BGP RT Background</code> there are (3) announcement bits to reflect the three clients (protocols) that have state for this route: Kernel (0-KRT), 5 (resolution tree process 2), and 8 (BGP).</td>
</tr>
<tr>
<td></td>
<td>The notation <code>n-Resolve inet</code> indicates that the route is used for route resolution for next hops found in the routing table. <code>n</code> is an index used by Juniper Networks customer support only.</td>
</tr>
</tbody>
</table>
Table 102: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS path</td>
<td>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
</tr>
<tr>
<td></td>
<td>• Recorded—The AS path is recorded by the sample process (sampled).</td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
</tr>
<tr>
<td></td>
<td>When AS path numbers are included in the route, the format is as follows:</td>
</tr>
<tr>
<td></td>
<td>• [ ]—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured.</td>
</tr>
<tr>
<td></td>
<td>• { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.</td>
</tr>
<tr>
<td></td>
<td>• ( )—Parentheses enclose a confederation.</td>
</tr>
<tr>
<td></td>
<td>• ( [ ] )—Parentheses and brackets enclose a confederation set.</td>
</tr>
<tr>
<td>validation-state</td>
<td>(BGP-learned routes) Validation status of the route:</td>
</tr>
<tr>
<td></td>
<td>• Invalid—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database.</td>
</tr>
<tr>
<td></td>
<td>• Unverified—Indicates that origin validation is not enabled for the BGP peers.</td>
</tr>
<tr>
<td></td>
<td>• Valid—Indicates that the prefix and autonomous system pair are found in the database.</td>
</tr>
<tr>
<td>FECs bound to route</td>
<td>Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.</td>
</tr>
<tr>
<td>AS path: I &lt;Originator&gt;</td>
<td>(For route reflected output only) Originator ID attribute set by the route reflector.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>route status</td>
<td>Indicates the status of a BGP route:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Accepted</strong>—The specified BGP route is imported by the default BGP policy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Import</strong>—The route is imported into a Layer 3 VPN routing instance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Import-Protect</strong>—A remote instance egress that is protected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multipath</strong>—A BGP multipath active route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MultipathContrib</strong>—The route is not active but contributes to the BGP multipath.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Protect</strong>—An egress route that is protected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stale</strong>—A route that is marked stale due to graceful restart.</td>
</tr>
<tr>
<td>Primary Upstream</td>
<td>When multipoint LDP with multicast-only fast reroute (MoFRR) is configured, the primary upstream path. MoFRR transmits a multicast join message from a receiver toward a source on a primary path, while also transmitting a secondary multicast join message from the receiver toward the source on a backup path.</td>
</tr>
<tr>
<td>RPF Nexthops</td>
<td>When multipoint LDP with MoFRR is configured, the reverse-path forwarding (RPF) next-hop information. Data packets are received from both the primary path and the secondary paths. The redundant packets are discarded at topology merge points due to the RPF checks.</td>
</tr>
<tr>
<td>Label</td>
<td>Multiple MPLS labels are used to control MoFRR stream selection. Each label represents a separate route, but each references the same interface list check. Only the primary label is forwarded while all others are dropped. Multiple interfaces can receive packets using the same label.</td>
</tr>
<tr>
<td>weight</td>
<td>Value used to distinguish MoFRR primary and backup routes. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</td>
</tr>
<tr>
<td>VC Label</td>
<td>MPLS label assigned to the Layer 2 circuit virtual connection.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN identifier of the Layer 2 circuit.</td>
</tr>
<tr>
<td>Cluster list</td>
<td>(For route reflected output only) Cluster ID sent by the route reflector.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>(For route reflected output only) Address of router that originally sent the route to the route reflector.</td>
</tr>
<tr>
<td>Prefixes bound to route</td>
<td>Forwarding Equivalent Class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
</tbody>
</table>
Table 102: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See the Output Field table in the <code>show route detail</code> command for all possible values for this field.</td>
</tr>
<tr>
<td>Layer2-info:encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
</tr>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) information.</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.</td>
</tr>
<tr>
<td>status vector</td>
<td>Layer 2 VPN and VPLS network layer reachability information (NLRI).</td>
</tr>
<tr>
<td>Localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>Router ID</td>
<td>BGP router ID as advertised by the neighbor in the open message.</td>
</tr>
<tr>
<td>Primary Routing</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</td>
</tr>
<tr>
<td>Table</td>
<td></td>
</tr>
<tr>
<td>Secondary Tables</td>
<td>In a routing table group, the name of one or more secondary tables in which the route resides.</td>
</tr>
<tr>
<td>Originating RIB</td>
<td>Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.</td>
</tr>
<tr>
<td>Node path count</td>
<td>Number of nodes in the path.</td>
</tr>
<tr>
<td>Forwarding nexthops</td>
<td>Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.</td>
</tr>
</tbody>
</table>

Sample Output

```
show route extensive

user@host>  show route extensive
```
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
203.0.113.10/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.10/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 29
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 64496
  Age: 1:34:06
  Task: RT
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

203.0.113.30/30 (2 entries, 1 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 2
  Next hop: via so-0/3/0.0, selected
  State: <Active Int>
  Local AS: 64496
  Age: 1:32:40
  Task: IF
  Announcement bits (1): 3-Resolve tree 2
  AS path: I
  OSPF Preference: 10
  Next-hop reference count: 1
  Next hop: via so-0/3/0.0, selected
  State: <Int>
  Inactive reason: Route Preference
  Local AS: 64496
  Age: 1:32:40
  Metric: 1
  Area: 0.0.0.0
  Task: OSPF
  AS path: I

203.0.113.103/32 (1 entry, 1 announced)
  *Local Preference: 0
  Next hop type: Local
  Next-hop reference count: 7
  Interface: so-0/3/0.0
  State: <Active NoReadvrt Int>
  Local AS: 644969
  Age: 1:32:43
Task: IF
Announcement bits (1): 3-Resolve tree 2
AS path: I

...

203.0.113.203/30 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.203/30 -> {203.0.113.216}
   *OSPF   Preference: 10
   Next-hop reference count: 9
   Next hop: via so-0/3/0.0
   Next hop: 203.0.113.216 via ge-3/1/0.0, selected
   State: <Active Int>
   Local AS:  64496
   Age: 1:32:19   Metric: 2
   Area: 0.0.0.0
   Task: OSPF
   Announcement bits (2): 0-KRT 3-Resolve tree 2
   AS path: I

...

198.51.100.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 198.51.100.2/32 -> {}  
   *PIM   Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS:  64496
   Age: 1:34:08
   Task: PIM Recv
   Announcement bits (2): 0-KRT 3-Resolve tree 2
   AS path: I

...

198.51.100.22/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 198.51.100.22/32 -> {} 
   *IGMP   Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS:  64496
Age: 1:34:06
Task: IGMP
Announcement bits (2): 0-KRT 3-Resolve tree 2
AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

203.0.113.103/32 (1 entry, 1 announced)
  State: <FlashAll>
    *RSVP  Preference: 7
    Next-hop reference count: 6
    Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1, selected
    Label-switched-path green-r1-r3
    Label operation: Push 100096
    State: <Active Int>
    Local AS:  64496
    Age: 1:28:12    Metric: 2
    Task: RSVP
    Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
    AS path: I

203.0.113.238/32 (1 entry, 1 announced)
  State: <FlashAll>
    *RSVP  Preference: 7
    Next-hop reference count: 6
    Next hop: via so-0/3/0.0 weight 0x1, selected
    Label-switched-path green-r1-r2
    State: <Active Int>
    Local AS:  64496
    Age: 1:28:12    Metric: 1
    Task: RSVP
    Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
    AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
...

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
Next hop: via lo0.0, selected
State: <Active Int>
Local AS: 64496
Age: 1:34:07
Task: IF
AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0 (1 entry, 1 announced)
TSI:
KRT in-kernel 0 /36 -> {}
   *MPLS Preference: 0
    Next hop type: Receive
    Next-hop reference count: 6
    State: <Active Int>
    Local AS: 64496
    Age: 1:34:08 Metric: 1
    Task: MPLS
    Announcement bits (1): 0-KRT
    AS path: I

...
Next hop: 198.51.100.2 via lt-1/2/0.5 weight 0x8001
Label operation: Pop
State: <Active Int>
Age: 1:29 Metric: 1
Task: RSVP
Announcement bits (1): 0-KRT
AS path: I...

800010 (1 entry, 1 announced)

TSI:
KRT in-kernel 800010 /36 -> (vt-3/2/0.32769)
    *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: via vt-3/2/0.32769, selected
    Label operation: Pop
    State: <Active Int>
    Age: 1:31:53
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)
TSI:
KRT in-kernel vt-3/2/0.32769.0 /16 -> (indirect(1048574))
    *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1, selected
    Label-switched-path green-r1-r3
    Label operation: Push 800012, Push 100096(top)
    Protocol next hop: 203.0.113.103
    Push 800012
    Indirect next hop: 87272e4 1048574
    State: <Active Int>
    Age: 1:31:53 Metric2: 2
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 1-Common L2 VC
    AS path: I
    Communities: target:11111:1 Layer2-info: encaps:VPLS,
                  control flags:, mtu: 0
    Indirect next hops: 1
    Protocol next hop: 203.0.113.103 Metric: 2
    Push 800012
    Indirect next hop: 87272e4 1048574
Indirect path forwarding next hops: 1
    Next hop: 203.0.113.216 via ge-3/1/0.0 weight 0x1

203.0.113.103/32 Originating RIB: inet.3
    Metric: 2                  Node path count: 1
    Forwarding nexthops: 1
    Nexthop: 203.0.113.216 via ge-3/1/0.0

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

2001:db8::10:255:71:52/128 (1 entry, 0 announced)
    *Direct Preference: 0
    Next hop type: Interface
    Next-hop reference count: 1
    Next hop: via lo0.0, selected
    State: <Active Int>
    Local AS: 64496
    Age: 1:34:07
    Task: IF
    AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
    *Direct Preference: 0
    Next hop type: Interface
    Next-hop reference count: 1
    Next hop: via lo0.0, selected
    State: <Active NoReadvrt Int>
    Local AS: 64496
    Age: 1:34:07
    Task: IF
    AS path: I

ff02::2/128 (1 entry, 1 announced)
    TSI:
    KRT in-kernel ff02::2/128 -> {}
    *PIM Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 64496
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I
ff02::d/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::d/128 -> {}
   *PIM Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS:  64496
   Age: 1:34:08
   Task: PIM Recv6
   Announcement bits (1): 0-KRT
   AS path: I

ff02::16/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::16/128 -> {}
   *MLD Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS:  64496
   Age: 1:34:06
   Task: MLD
   Announcement bits (1): 0-KRT
   AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
   *Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 1
   Next hop: via lo0.16385, selected
   State: <Active NoReadvrt Int>
   Age: 1:34:07
   Task: IF
   AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

203.0.113.103:1:3:1/96 (1 entry, 1 announced)
   *BGP Preference: 170/-101
   Route Distinguisher: 203.0.113.103:1
   Next-hop reference count: 7
   Source: 203.0.113.103
   Protocol next hop: 203.0.113.103
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS:    64496 Peer AS:    64496
Age: 1:28:12    Metric2: 1
Task: BGP_69.203.0.113.103+179
Announcement bits (1): 0-green-12vpn
AS path: I
Communities: target:11111:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0
Label-base: 800008, range: 8
Localpref: 100
Router ID: 203.0.113.103
Primary Routing Table bgp.12vpn.0

203.0.113.152:1:1:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699540
  *L2VPN  Preference: 170/-1
  Next-hop reference count: 5
  Protocol next hop: 203.0.113.152
  Indirect next hop: 0 -
  State: <Active Int Ext>
  Age: 1:34:03    Metric2: 1
  Task: green-12vpn
  Announcement bits (1): 1-BGP.0.0.0.0+179
  AS path: I
  Communities: Layer2-info: encaps:VPLS, control flags:Site-Down, mtu: 0
  Label-base: 800016, range: 8, status-vector: 0x9F

203.0.113.152:1:5:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699528
  *L2VPN  Preference: 170/-101
  Next-hop reference count: 5
  Protocol next hop: 203.0.113.152
  Indirect next hop: 0 -
  State: <Active Int Ext>
  Age: 1:34:03    Metric2: 1
  Task: green-12vpn
  Announcement bits (1): 1-BGP.0.0.0.0+179
  AS path: I
  Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
  Label-base: 800008, range: 8, status-vector: 0x9F
l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

203.0.113.163:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT  Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
    Label operation: Push 100000[0]
    Protocol next hop: 203.0.113.163 Indirect next hop: 86af000 296
    State: <Active Int>
    Local AS: 64499
    Age: 10:21
    Task: 12 circuit
    Announcement bits (1): 0-LDP
    AS path: I
    VC Label 100000, MTU 1500, VLAN ID 512

203.0.113.55/24 (1 entry, 1 announced)
TSI:
KRT queued (pending) add
  198.51.100.0/24 -> {Push 300112}
  *BGP  Preference: 170/-101
    Next hop type: Router
    Address: 0x925c208
    Next-hop reference count: 2
    Source: 203.0.113.9
    Next hop: 203.0.113.9 via ge-1/2/0.15, selected
    Label operation: Push 300112
    Label TTL action: prop-ttl
    State: <Active Ext>
    Local AS: 64509 Peer AS: 65539
    Age: 1w0d 23:06:56
    AIGP: 25
    Task: BGP_65539.203.0.113.9+56732
    Announcement bits (1): 0-KRT
    AS path: 65539 64508 I
    Accepted
    Route Label: 300112
show route extensive (Access Route)

user@host> show route 203.0.113.102 extensive

inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
203.0.113.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 203.0.113.102/32 -> {192.0.2.2}
OSPF area : 0.0.0.0, LSA ID : 203.0.113.102, LSA type : Extern
  *Access Preference: 13
    Next-hop reference count: 78472
    Next hop: 192.0.2.2 via fe-0/0/0.0, selected
    State: <Active Int>
Age: 12
  Task: RPD Unix Domain Server./var/run/rpd_serv.local
Announcement bits (2): 0-KRT 1-OSPFv2
AS path: I

user@host> show route 2001:db8:4641:1::/48 extensive

inet6.0: 75 destinations, 81 routes (75 active, 0 holddown, 0 hidden)
2001:db8:4641:1::/48 (1 entry, 1 announced)
TSI:
KRT in-kernel 2001:db8:4641:1::/48 -> {#0 0.13.1.0.0.1}
  *Access Preference: 13
    Next hop type: Router, Next hop index: 74548
    Address: 0x1638c1d8
    Next-hop reference count: 6
    Next hop: #0 0.13.1.0.0.1 via demux0.1073753267, selected
    Session Id: 0x0
    State: <Active Int>
    Age: 4:17
    Validation State: unverified
    Task: RPD Unix Domain Server./var/run/rpd_serv.local
  Announcement bits (2): 0-KRT 4-Resolve tree 2
AS path: I
2001:db8:4641:1::/128 (1 entry, 1 announced)
TSI:
KRT in-kernel 2001:db8:4641:1::/128 -> {#0 0.13.1.0.0.1}
  *Access-internal Preference: 12
  Next hop type: Router, Next hop index: 74548
  Address: 0x1638c1d8
  Next-hop reference count: 6
  Next hop: #0 0.13.1.0.0.1 via demux0.1073753267, selected
  Session Id: 0x0
  State: <Active Int>
  Age: 4:17
  Validation State: unverified
  Task: RPD Unix Domain Server./var/run/rpd_serv.local
  Announcement bits (2): 0-KRT 4-Resolve tree 2
  AS path: I

show route extensive (BGP PIC Edge)

`user@host> show route 198.51.100.6 extensive`

ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
  198.51.100.6/32 (3 entries, 2 announced)
    State: <CalcForwarding>
    TSI:
    KRT in-kernel 198.51.100.6/32 -> {indirect(1048574), indirect(1048577)}
    Page 0 idx 0 Type 1 val 9219e30
      Nexthop: Self
      AS path: [2] 3 I
      Communities: target:2:1
      Path 198.51.100.6 from 198.51.100.4 Vector len 4. Val: 0
    ...
      #Multipath Preference: 255
      Next hop type: Indirect
      Address: 0x93f4010
      Next-hop reference count: 2
    ...
      Protocol next hop: 198.51.1001.4
      Push 299824
      Indirect next hop: 944c000 1048574 INH Session ID: 0x3
      Indirect next hop: weight 0x1
      Protocol next hop: 198.51.100.5
      Push 299824
      Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
      Indirect next hop: weight 0x4000
      State: <ForwardingOnly Int Ext>
      Inactive reason: Forwarding use only
show route extensive (FRR and LFA)

user@host> show route 203.0.113.20 extensive

inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
203.0.113.20/24 (2 entries, 1 announced)
    State: FlashAll
TSI:
KRT in-kernel 203.0.113.20/24 -> {Push 299776, Push 299792}
    *RSVP    Preference: 7/1
    Next hop type: Router, Next hop index: 1048576
    Address: 0xbbbc010
    Next-hop reference count: 5
    Next hop: 203.0.113.112 via ge-2/1/8.0 weight 0x1, selected
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299776
    Label TTL action: prop-ttl
    Session Id: 0x201
    Next hop: 203.0.113.122 via ge-2/1/4.0 weight 0x4001
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299792
    Label TTL action: prop-ttl
    Session Id: 0x202
    State: Active Int
    Local AS:   64500
    Age: 5:31  Metric: 2
    Task: RSVP
    Announcement bits (1): 0-KRT
    AS path: I
OSPFP     Preference: 10
    Next hop type: Router, Next hop index: 615
    Address: 0xb9d78c4
    Next-hop reference count: 7
    Next hop: 203.0.113.112 via ge-2/1/8.0, selected
    Session Id: 0x201
    State: Int
    Inactive reason: Route Preference
Local AS: 64500
Age: 5:35 Metric: 3
Area: 0.0.0.0
Task: OSPF
AS path: I

**show route extensive (IS-IS)**

```
user@host> show route extensive

IS-IS Preference: 15
   Level: 1
   Next hop type: Router, Next hop index: 1048577
   Address: 0xxxxxxxxxx
   Next-hop reference count: YY
   Next hop: 203.0.113.22 via ae1.0 balance 43%, selected
   Session Id: 0x141
   Next hop: 203.0.113.22 via ae0.0 balance 57%
```

**show route extensive (Route Reflector)**

```
user@host> show route extensive

203.0.113.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 203.0.113.0/8 -> {indirect(40)}
   *BGP   Preference: 170/-101
   Source: 192.168.4.214
   Protocol next hop: 198.51.100.192 Indirect next hop: 84ac908 40
   State: <Active Int Ext>
   Local AS: 65548 Peer AS: 65548
   Age: 3:09 Metric: 0 Metric2: 0
   Task: BGP_65548.192.168.4.214+1033
   Announcement bits (2): 0-KRT 4-Resolve inet.0
   AS path: 6544 64507 I <Originator>
   Cluster list: 198.51.100.1
   Originator ID: 203.0.113.48
   Communities: 7777:7777
   Localpref: 100
   Router ID: 203.0.113.4
   Indirect next hops: 1
      Protocol next hop: 203.0.113.192 Metric: 0
```
Indirect next hop: 84ac908 40
Indirect path forwarding next hops: 0
Next hop type: Discard

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show route label 299872 detail

mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
   *LDP  Preference: 9
   Next hop type: Flood
   Next-hop reference count: 3
   Address: 0x9097d90
   Next hop: via vt-0/1/0.1
   Next-hop index: 661
   Label operation: Pop
   Address: 0x9172130
   Next hop: via so-0/0/3.0
   Next-hop index: 654
   Label operation: Swap 299872
   State: **Active Int>
   Local AS:  64511
   Age: 8:20       Metric: 1
   Task: LDP
   Announcement bits (1): 0-KRT
   AS path: I
   FECs bound to route: P2MP root-addr 203.0.113.166, grp 203.0.113.1, src 192.168.142.2

show route label detail (Multipoint LDP with Multicast-Only Fast Reroute)

user@host> show route label 301568 detail

mpls.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
301568 (1 entry, 1 announced)
   *LDP  Preference: 9
   Next hop type: Flood
   Address: 0x2735208
   Next-hop reference count: 3
   Next hop type: Router, Next hop index: 1397
   Address: 0x2735d2c
Next-hop reference count: 3
Next hop: 203.0.113.82 via ge-1/2/22.0
Label operation: Pop
Load balance label: None;
Next hop type: Router, Next hop index: 1395
Address: 0x2736290
Next-hop reference count: 3
Next hop: 203.0.113.2 via ge-1/2/18.0
Label operation: Pop
Load balance label: None;
State: <Active Int AckRequest MulticastRPF>
Local AS: 64500
Age: 54:05 Metric: 1
Validation State: unverified
Task: LDP
Announcement bits (1): 0-KRT
AS path: I
FECS bound to route: P2MP root-addr 198.51.100.1, grp: 203.0.113.1, src: 192.168.219.11
Primary Upstream : 198.51.100.3:0--198.51.100.2:0
RPF Nexthops :
  ge-1/2/15.0, 10.2.94.1, Label: 301568, weight: 0x1
  ge-1/2/14.0, 10.2.3.1, Label: 301568, weight: 0x1
Backup Upstream : 198.51.100.3:0--198.51.100.6:0
RPF Nexthops :
  ge-1/2/20.0, 198.51.100.96, Label: 301584, weight: Oxfffe
  ge-1/2/19.0, 198.51.100.36, Label: 301584, weight: Oxfffe

show route extensive (Flexible VXLAN Tunnel Profile)

user@host> show route 192.168.0.2 extensive

... CUSTOMER_0001.inet.0: 5618 destinations, 6018 routes (5618 active, 0 holddown, 0 hidden)

192.168.0.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.0.2/32 -> {fti0.6 Flags NSR-incapable}
Opaque data client: FLEX-TNL
Address: 0xd00eee8
Opaque data reference count: 2
Opaque data: Flexible IPv6 VXLAN tunnel profile
*Static Preference: 5/100
   Next hop type: Router, Next hop index: 74781
   Address: 0x5d9b03cc
   Next-hop reference count: 363
   Next hop: via fti0.6, selected
   Session Id: 0x24c8
   State: <Active Int NSR-incapable OpaqueData Programmed>
   Age: 1:34:00
   Validation State: unverified
      Tag: 10000001   Tag2: 1
   Announcement bits (2): 1-KRT 3-Resolve tree 30
   AS path: I
   Flexible IPv6 VXLAN tunnel profile
      Action: Encapsulate
      Interface: fti0.6 (Index: 10921)
      VNI: 10000001
      Source Prefix: 2001:db8:255::2/128
      Source UDP Port Range: 54614 - 60074
      Destination Address: 2001:db8:80:1:1:1:0:1
      Destination UDP Port: 4790
      VXLAN Flags: 0x08
...
show route instance

Syntax

show route instance
   <brief | detail | summary>
   <instance-name>
   <operational>

Release Information
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
(QFabric systems only) Display routing instance information.

Options

none—(Same as brief) Display standard information about all routing instances.

brief | detail | summary—(Optional) Display the specified level of output. If you do not specify a level of 
output, the system defaults to brief. (These options are not available with the operational keyword.)

instance-name—(Optional) Display information for a specified routing instance.

operational—(Optional) Display operational routing instances.

Required Privilege Level
view

List of Sample Output
show route instance on page 2754
show route instance detail on page 2755
show route instance operational on page 2756
show route instance summary on page 2756

Output Fields
Table 103 on page 2753 lists the output fields for the show route instance command. Output fields are listed 
in the approximate order in which they appear.

Table 103: show route instance Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance or instance-name</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 103: show route instance Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Routing Instances</strong></td>
<td>(operational keyword only) Names of all operational routing instances.</td>
<td>—</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of routing instance: forwarding or virtual-router.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>State of the routing instance: active or inactive.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>Name of interfaces belonging to this routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Tables</strong></td>
<td>Tables (and number of routes) associated with this routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Router ID</strong></td>
<td>Identifier for the router.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Primary RIB</strong></td>
<td>Primary table for this routing instance.</td>
<td>brief none summary</td>
</tr>
<tr>
<td><strong>Active/holddown/hidden</strong></td>
<td>Number of active, hold-down, and hidden routes.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

```plaintext
show route instance

user@switch>  show route instance

<table>
<thead>
<tr>
<th>Instance</th>
<th>Type</th>
<th>Primary RIB</th>
<th>Active/holddown/hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>forwarding</td>
<td>inet.0</td>
<td>4/0/1</td>
</tr>
<tr>
<td><strong>juniper_private1</strong> forwarding</td>
<td><strong>juniper_private1</strong>.inet.0</td>
<td></td>
<td>1/0/3</td>
</tr>
<tr>
<td><strong>juniper_private2</strong> forwarding</td>
<td><strong>juniper_private2</strong>.inet.0</td>
<td></td>
<td>0/0/1</td>
</tr>
<tr>
<td><strong>juniper_private3</strong> forwarding</td>
<td><strong>juniper_private3</strong>.inet.0</td>
<td></td>
<td>1/0/2</td>
</tr>
<tr>
<td><strong>juniper_private4</strong> forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show route instance detail

user@switch> show route instance detail

master:
  Router ID: 10.3.3.7
  Type: forwarding        State: Active
  Tables:
    inet.0                 : 5 routes (4 active, 0 holddown, 1 hidden)

__juniper_private1__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16385
    bme0.0
  Tables:
    __juniper_private1__.inet.0: 6 routes (1 active, 0 holddown, 3 hidden)

__juniper_private2__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    lo0.16384
  Tables:
    __juniper_private2__.inet.0: 1 routes (0 active, 0 holddown, 1 hidden)

__juniper_private3__:
  Router ID: 0.0.0.0
  Type: forwarding        State: Active
  Interfaces:
    bme0.1
  Tables:
    __juniper_private3__.inet.0: 4 routes (1 active, 0 holddown, 2 hidden)

__juniper_private4__:
Router ID: 0.0.0.0
Type: forwarding    State: Active
Interfaces:
    bme0.2
Tables:
    __juniper_private4__.inet.0: 8 routes (4 active, 0 holddown, 2 hidden)

__master.anon__:
    Router ID: 0.0.0.0
    Type: forwarding    State: Active

r1:
    Router ID: 0.0.0.0
    Type: virtual-router    State: Active
    Interfaces:
        xe-0/0/0.0

r2:
    Router ID: 0.0.0.0
    Type: virtual-router    State: Active
    Interfaces:
        xe-0/0/3.0

**show route instance operational**

user@switch> **show route instance operational**

Operational Routing Instances:

    __juniper_private1__
    __juniper_private2__
    __juniper_private2__
    __juniper_private3__
    __juniper_private4__
    r1---qfabric
    r2---qfabric
    master

**show route instance summary**

user@switch> **show route instance summary**

<table>
<thead>
<tr>
<th>Instance</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary RIB</td>
<td>Active/holddown/hidden</td>
</tr>
</tbody>
</table>
master               forwarding
    inet.0             4/0/1

__juniper_private1__ forwarding
    __juniper_private1__.inet.0  1/0/3

__juniper_private2__ forwarding
    __juniper_private2__.inet.0  0/0/1

__juniper_private3__ forwarding
    __juniper_private3__.inet.0  1/0/2

__juniper_private4__ forwarding
    __juniper_private4__.inet.0  4/0/2

__master.anon__      forwarding

r1                 virtual-router
r2                 virtual-router
show route protocol

List of Syntax
Syntax on page 2758
Syntax (EX Series Switches) on page 2758

Syntax

show route protocol protocol
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route protocol protocol
  <brief | detail | extensive | terse>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
ospf2 and ospf3 options introduced in Junos OS Release 9.2.
ospf2 and ospf3 options introduced in Junos OS Release 9.2 for EX Series switches.
flow option introduced in Junos OS Release 10.0.
flow option introduced in Junos OS Release 10.0 for EX Series switches.

Description
Display the route entries in the routing table that were learned from a particular protocol.

Options
brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

protocol—Protocol from which the route was learned:

- access—Access route for use by DHCP application
- access-internal—Access-internal route for use by DHCP application
- aggregate—Locally generated aggregate route
- arp—Route learned through the Address Resolution Protocol
• atmvpn—Asynchronous Transfer Mode virtual private network
• bgp—Border Gateway Protocol
• ccc—Circuit cross-connect
• direct—Directly connected route
• dvmrp—Distance Vector Multicast Routing Protocol
• eisis—End System-to-Intermediate System
• flow—Locally defined flow-specification route
• frr—Precomputed protection route or backup route used when a link goes down
• isis—Intermediate System-to-Intermediate System
• ldp—Label Distribution Protocol
• l2circuit—Layer 2 circuit
• l2vpn—Layer 2 virtual private network
• local—Local address
• mpls—Multiprotocol Label Switching
• msdp—Multicast Source Discovery Protocol
• ospf—Open Shortest Path First versions 2 and 3
• ospf2—Open Shortest Path First versions 2 only
• ospf3—Open Shortest Path First version 3 only
• pim—Protocol Independent Multicast
• rip—Routing Information Protocol
• ripng—Routing Information Protocol next generation
• rsvp—Resource Reservation Protocol
• rtarget—Local route target virtual private network
• static—Statically defined route
• tunnel—Dynamic tunnel
• vpn—Virtual private network

NOTE: EX Series switches run a subset of these protocols. See the switch CLI for details.

Required Privilege Level
List of Sample Output

*show route protocol access* on page 2760
*show route protocol access-internal extensive* on page 2761
*show route protocol arp* on page 2761
*show route protocol bgp* on page 2762
*show route protocol bgp detail* on page 2762
*show route protocol bgp detail (Labeled Unicast)* on page 2763
*show route protocol bgp detail (Aggregate Extended Community Bandwidth)* on page 2764
*show route protocol bgp extensive* on page 2765
*show route protocol bgp terse* on page 2766
*show route protocol direct* on page 2766
*show route protocol frr* on page 2766
*show route protocol l2circuit detail* on page 2768
*show route protocol l2vpn extensive* on page 2769
*show route protocol ldp* on page 2770
*show route protocol ldp extensive* on page 2770
*show route protocol ospf (Layer 3 VPN)* on page 2772
*show route protocol ospf detail* on page 2773
*show route protocol rip* on page 2773
*show route protocol rip detail* on page 2773
*show route protocol ripng table inet6* on page 2774
*show route protocol static detail* on page 2774

Output Fields

For information about output fields, see the output field tables for the *show route* command, the *show route detail* command, the *show route extensive* command, or the *show route terse* command.

---

Sample Output

*show route protocol access*

```
user@host> show route protocol access

inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

13.160.0.3/32    *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32    *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0
```
13.160.0.5/32 *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0

show route protocol access-internal extensive

user@host> show route protocol access-internal 13.160.0.19 extensive

inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
  *Access-internal Preference: 12
    Next-hop reference count: 200000
    Next hop: 13.160.0.2 via fe-0/0/0.0, selected
    State: <Active Int>
    Age: 36
    Task: RPD Unix Domain Server./var/run/rpd_serv.local
    Announcement bits (1): 0-KRT
    AS path: I

show route protocol arp

user@host> show route protocol arp

inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.4/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.5/32 [ARP/4294967293] 00:04:32, from 20.20.1.1
  Unusable
20.20.1.6/32 [ARP/4294967293] 00:04:34, from 20.20.1.1
  Unusable
20.20.1.7/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.8/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
show route protocol bgp

user@host> **show route protocol bgp** 192.168.64.0/21

inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.64.0/21  *[BGP/170]  6d 10:41:16, localpref 100, from 192.168.69.71
    AS path: 10458 14203 2914 4788 4788 I
        > to 192.168.167.254 via fxp0.0

show route protocol bgp detail

user@host> **show route protocol bgp** 66.117.63.0/24 detail

inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24  (1 entry, 1 announced)
   *BGP  Preference: 170/-101
       Next hop type: Indirect
       Next-hop reference count: 1006436
       Source: 192.168.69.71
       Next hop type: Router, Next hop index: 324
       Next hop: 192.168.167.254 via fxp0.0, selected
       Protocol next hop: 192.168.69.71
       Indirect next hop: 8e166c0 342
       State: <Active Ext>
       Local AS: 69 Peer AS: 10458
       Age: 6d 10:42:42  Metric2: 0
       Task: BGP_10458.192.168.69.71+179
       Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree 1
show route protocol bgp detail (Labeled Unicast)

inet.0: 45 destinations, 46 routes (45 active, 0 holddown, 0 hidden)
1.1.1.8/32 (2 entries, 2 announced)
State:
*BGP Preference: 1/-101
Next hop type: Indirect, Next hop index: 0
Address: 0xc007f30
Next-hop reference count: 2
Source: 1.1.1.1
Next hop type: Router, Next hop index: 614
Next hop: 20.1.1.2 via ge-0/0/1.0, selected
Label-switched-path lsp1
Label operation: Push 1000126, Push 1000125, Push 1000124, Push 1000123, Push 299872(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 1000126: None; Label 1000125: None; Label 1000124: None; Label 1000123: None; Label 299872: None;
Label element ptr: 0xc007860
Label parent element ptr: 0xc0089a0
Label element references: 1
Label element child references: 0
Label element lsp id: 0
Session Id: 0x140
Protocol next hop: 1.1.1.4
Label operation: Push 1000126, Push 1000125, Push 1000124, Push 1000123(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl, prop-ttl, prop-ttl
Load balance label: Label 1000126: None; Label 1000125: None; Label 1000124: None; Label 1000123: None;
Indirect next hop: 0xae8d300 1048576 INH Session ID: 0x142
State:
Local AS: 5 Peer AS: 5
Age: 22:43 Metric2: 2
Validation State: unverified
Task: BGP_5.1.1.1.1
Announcement bits (2): 0-KRT 7-Resolve tree 2
AS path: I
Accepted
Route Labels: 1000123(top) 1000124 1000125 1000126
Localpref: 100
Router ID: 1.1.1.1

show route protocol bgp detail (Aggregate Extended Community Bandwidth)

user@host> show route 10.0.2.0 protocol bgp detail

inet.0: 20 destinations, 26 routes (20 active, 0 holddown, 0 hidden)
10.0.2.0/30 (2 entries, 1 announced)
  *BGP    Preference: 170/-101
         Next hop type: Router, Next hop index: 0
         Address: 0xb618990
         Next-hop reference count: 3
         Source: 10.0.1.1
         Next hop: 10.0.0.2 via ge-0/0/0.0 balance 40%
         Session Id: 0x0
         Next hop: 10.0.1.1 via ge-0/0/1.0 balance 60%, selected
         Session Id: 0x0
         State: <Active Ext>
         Local AS: 65000 Peer AS: 65001
         Age: 20:33
         Validation State: unverified
         Task: BGP_65001.10.0.1.1
         Announcement bits (3): 0-KRT 2-BGP_Listen.0.0.0.0+179

3-BGP_RT_Background
  AS path: 65001 I
  Communities: bandwidth:65000:60000000
  Accepted Multipath
  Localpref: 100
  Router ID: 128.49.121.137
  BGP    Preference: 170/-101
         Next hop type: Router, Next hop index: 595
         Address: 0xb7a1330
         Next-hop reference count: 9
         Source: 10.0.0.2
         Next hop: 10.0.0.2 via ge-0/0/0.0, selected
         Session Id: 0x141
         State: <NotBest Ext>
         Inactive reason: Not Best in its group - Active preferred
         Local AS: 65000 Peer AS: 65001
         Age: 20:33
show route protocol bgp extensive

user@host> show route protocol bgp 192.168.64.0/21 extensive

inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21 (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
Next hop: Self
   AS path: [69] 10458 14203 2914 4788 4788 I
   Communities: 2914:410 2914:2403 2914:3400
Path 1.9.0.0 from 192.168.69.71 Vector len 4.  Val: 1
   *BGP    Preference: 170/-101
   Next hop type: Indirect
   Next-hop reference count: 1006502
   Source: 192.168.69.71
   Next hop type: Router, Next hop index: 324
   Next hop: 192.168.167.254 via fxp0.0, selected
   Protocol next hop: 192.168.69.71
   Indirect next hop: 8e166c0 342
   State: <Active Ext>
Local AS: 69 Peer AS: 10458
Age: 6d 10:44:45  Metric2: 0
Task: BGP_10458.192.168.69.71+179
Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree I

AS path: 10458 14203 2914 4788 4788 I
Communities: 2914:410 2914:2403 2914:3400
Accepted
Localpref: 100
Router ID: 207.17.136.192
Indirect next hops: 1
   Protocol next hop: 192.168.69.71
   Indirect next hop: 8e166c0 342
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 192.168.167.254 via fxp0.0
192.168.0.0/16 Originating RIB: inet.0
Node path count: 1
Forwarding nexthops: 1
Nexthop: 192.168.167.254 via fxp0.0

show route protocol bgp terse

user@host> show route protocol bgp 192.168.64.0/21 terse

inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.64.0/21</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>&gt;172.16.100.1</td>
<td>10023</td>
</tr>
</tbody>
</table>

show route protocol direct

user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>Destination</th>
<th>Route Type</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.8.0/24</td>
<td>[Direct/0]</td>
<td>17w0d</td>
<td></td>
<td></td>
<td>10:31:49</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via fe-1/3/1.0</td>
<td></td>
</tr>
<tr>
<td>10.255.165.1/32</td>
<td>[Direct/0]</td>
<td>25w4d</td>
<td></td>
<td></td>
<td>04:13:18</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via lo0.0</td>
<td></td>
</tr>
<tr>
<td>172.16.30.0/24</td>
<td>[Direct/0]</td>
<td>17w0d</td>
<td></td>
<td></td>
<td>23:06:26</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via fe-1/3/2.0</td>
<td></td>
</tr>
<tr>
<td>192.168.164.0/22</td>
<td>[Direct/0]</td>
<td>25w4d</td>
<td></td>
<td></td>
<td>04:13:20</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via fxp0.0</td>
<td></td>
</tr>
</tbody>
</table>

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>Destination</th>
<th>Route Type</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152</td>
<td>[Direct/0]</td>
<td>25w4d</td>
<td></td>
<td></td>
<td>04:13:21</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via lo0.0</td>
<td></td>
</tr>
</tbody>
</table>
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:db8::10:255:165:1/128
    *[Direct/0] 25w4d 04:13:21
    > via lo0.0
fe80::2a0:a5ff:fe12:ad7/128
    *[Direct/0] 25w4d 04:13:21
    > via lo0.0

show route protocol frr

user@host> show route protocol frr

inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32    *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.3 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.4/32    *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.4 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.5/32    *[FRR/200] 00:05:35, from 20.20.1.1
    > to 20.20.1.5 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.6/32    *[FRR/200] 00:05:37, from 20.20.1.1
    > to 20.20.1.6 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.7/32    *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.7 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.8/32    *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.8 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.9/32    *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.9 via ge-4/1/0.0
    to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.10/32   *[FRR/200] 00:05:38, from 20.20.1.1
    ...
show route protocol l2circuit detail

user@host> show route protocol l2circuit detail

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
100000 (1 entry, 1 announced)
   *L2CKT  Preference: 7
   Next hop: via ge-2/0/0.0, selected
   Label operation: Pop  Offset: 4
   State: <Active Int>
   Local AS:  99
   Age: 9:52
   Task: Common L2 VC
   Announcement bits (1): 0-KRT
   AS path: I

ge-2/0/0.0 (1 entry, 1 announced)
   *L2CKT  Preference: 7
   Next hop: via so-1/1/2.0 weight 1, selected
   Label-switched-path my-lsp
   Label operation: Push 100000, Push 100000(top)[0] Offset: -4
   Protocol next hop: 10.245.255.63
   Push 100000 Offset: -4
   Indirect next hop: 86af0c0 298
   State: <Active Int>
   Local AS:  99
   Age: 9:52
   Task: Common L2 VC
   Announcement bits (2): 0-KRT 1-Common L2 VC
   AS path: I

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
   *L2CKT  Preference: 7
   Next hop: via so-1/1/2.0 weight 1, selected
   Label-switched-path my-lsp
   Label operation: Push 100000[0]
   Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
   State: <Active Int>
   Local AS:  99
   Age: 10:21
   Task: l2电路
   Announcement bits (1): 0-LDP
show route protocol l2vpn extensive

user@host> show route protocol l2vpn extensive

inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)
inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
800001 (1 entry, 1 announced)
TSI:
KRT in-kernel 800001 /36 -> (so-0/0/0.0)
   *L2VPN Preference: 7
       Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
       Label operation: Pop Offset: 4
       State: <Active Int>
       Local AS: 69
       Age: 7:48
       Task: Common L2 VC
       Announcement bits (1): 0-KRT
       AS path: I

so-0/0/0.0 (1 entry, 1 announced)
TSI:
KRT in-kernel so-0/0/0.0.0 /16 -> (indirect(288))
   *L2VPN Preference: 7
       Next hop: via so-0/0/1.0, selected
       Label operation: Push 800000 Offset: -4
       Push 800000 Offset: -4
       Indirect next hop: 85142a0 288
       State: <Active Int>
       Local AS: 69
       Age: 7:48
       Task: Common L2 VC
       Announcement bits (2): 0-KRT 1-Common L2 VC
       AS path: I
show route protocol ldp

inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1/32    *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Push 100000
192.168.17.1/32    *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100064             *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Pop
100064(S=0)        *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Pop
100080             *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Swap 100000

show route protocol ldp extensive

192.168.16.1/32 (1 entry, 1 announced)
State: <FlashAll>
  *LDP  Preference: 9
  Next-hop reference count: 3
  Next hop: via t1-4/0/0.0, selected
  Label operation: Push 100000
  State: <Active Int>
  Local AS: 64500
  Age: 1d 23:03:58    Metric: 1
  Task: LDP
Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
AS path: I

192.168.17.1/32 (1 entry, 1 announced)
  State: <FlashAll>
  *LDP  Preference: 9
  Next-hop reference count: 3
  Next hop: via t1-4/0/0.0, selected
  State: <Active Int>
  Local AS: 64500
  Age: 1d 23:03:58  Metric: 1
  Task: LDP
  Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
  AS path: I

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)

100064 (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /36 -> (t1-4/0/0.0)
  *LDP  Preference: 9
  Next-hop reference count: 2
  Next hop: via t1-4/0/0.0, selected
  State: <Active Int>
  Local AS: 64500
  Age: 1d 23:03:58  Metric: 1
  Task: LDP
  Announcement bits (1): 0-KRT
  AS path: I
  Prefixes bound to route: 192.168.17.1/32

100064(S=0) (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /40 -> (t1-4/0/0.0)
  *LDP  Preference: 9
  Next-hop reference count: 2
  Next hop: via t1-4/0/0.0, selected
  Label operation: Pop
  State: <Active Int>
  Local AS: 64500
  Age: 1d 23:03:58  Metric: 1
  Task: LDP
 show route protocol ospf (Layer 3 VPN)

user@host> show route protocol ospf

inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30  *[OSPF/10] 00:05:18, metric 4
> via t3-3/2/0.0
10.39.1.8/30  *[OSPF/10] 00:05:18, metric 2
> via t3-3/2/0.0
10.255.14.171/32 *[OSPF/10] 00:05:18, metric 4
> via t3-3/2/0.0
10.255.14.179/32 *[OSPF/10] 00:05:18, metric 2
> via t3-3/2/0.0
172.16.233.5/32  *[OSPF/10] 20:25:55, metric 1

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30  [OSPF/10] 00:05:43, metric 1
> via so-0/2/2.0
10.255.14.173/32 *[OSPF/10] 00:05:43, metric 1
> via so-0/2/2.0
172.16.233.5/32  *[OSPF/10] 20:26:20, metric 1
show route protocol ospf detail

user@host> show route protocol ospf detail

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
  OSPF Preference: 10
  Nexthop: via so-0/2/2.0, selected
  State: <Int>
  Inactive reason: Route Preference
  Age: 6:25 Metric: 1
  Area: 0.0.0.0
  Task: VPN-AB-OSPF
  AS path: I
  Communities: Route-Type:0.0.0.0:1:0

...

show route protocol rip

user@host> show route protocol rip

inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.14.177/32 *[RIP/100] 20:24:34, metric 2
  > to 10.39.1.22 via t3-0/2/2.0

172.16.233.9/32 *[RIP/100] 00:03:59, metric 1

show route protocol rip detail

user@host> show route protocol rip detail

inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.14.177/32 (1 entry, 1 announced)
  *RIP Preference: 100
**show route protocol ripng table inet6**

```
user@host> show route protocol ripng table inet6

inet6.0: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::2/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::3/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::4/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::5/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::6/128        *[RIPng/100] 02:13:33, metric 2
   > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
```

**show route protocol static detail**

```
user@host> show route protocol static detail

inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
10.5.0.0/16 (1 entry, 1 announced)
   *Static Preference: 5
   Next hop type: Router, Next hop index: 324
   Address: 0x9274010
   Next-hop reference count: 27
   Next hop: 192.168.187.126 via fxp0.0, selected
   Session Id: 0x0
   State: <Active NoReadvrt Int Ext>
   Age: 7w3d 21:24:25
   Validation State: unverified
```
Task: RT
Announcement bits (1): 0-KRT
AS path: I

10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.13.10.0/23 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I
show security ssh key-pair-identity

Syntax

show security ssh key-pair-identity
    ( brief <identity-name> | public identity-name )

Release Information
Command introduced in Junos OS Release 15.1X49-D70.

Description
Display the SSH key pair identity information.

Options
- **brief identity-name** — Display the brief information for a specified identity. The *identity-name* variable is optional, if an identity is not specified, the command will list brief information of all identities.
- **public identity-name** — Display the public key for a specified identity.

NOTE: The public and brief options are mutually exclusive

Required Privilege Level
view

RELATED DOCUMENTATION
request security ssh key-pair-identity generate | 2515
clear security ssh key-pair-identity | 2488

List of Sample Output
show security ssh key-pair-identity brief on page 2777
show security ssh key-pair-identity brief sample on page 2777

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

show security ssh key-pair-identity brief

user@host> show security ssh key-pair-identity brief

SSH Key Pair Identity Information:
Name           Create Time  Encrypted
sample         Dec 28, 17:40  yes
identity-name  Dec 28, 17:26  yes

show security ssh key-pair-identity brief sample

user@host> show security ssh key-pair-identity brief sample

SSH Key Pair Identity Information:
Name           Create Time  Encrypted
sample         Dec 28, 17:34  yes
show security pki local-certificate

Syntax

```
show security pki local-certificate
  <brief | detail>
  <certificate-id certificate-id-name>
  <system-generated>
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Display information about the local digital certificates and the corresponding public keys installed in the switch.

Options

none—(Same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display information about local digital certificates and corresponding public keys for the specified level of output.

certificate-id certificate-id-name—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.

system-generated—(Optional) Display information about the automatically generated self-signed certificate.

Required Privilege Level

view

RELATED DOCUMENTATION

| Manually Generating Self-Signed Certificates on Switches (CLI Procedure) | 345 |

List of Sample Output

- show security pki local-certificate on page 2780
- show security pki local-certificate detail on page 2780

Output Fields

Table 104 on page 2779 lists the output fields for the show security pki local-certificate command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate identifier</td>
<td>Name of the digital certificate.</td>
<td>All levels</td>
</tr>
<tr>
<td>Certificate version</td>
<td>Revision number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Issued by</td>
<td>Authority that issued the digital certificate.</td>
<td>none brief</td>
</tr>
<tr>
<td>Issued to</td>
<td>Device that was issued the digital certificate.</td>
<td>none brief</td>
</tr>
</tbody>
</table>
| Issuer              | Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:  
  - **Common name**—Name of the authority.  
  - **Organization**—Organization of origin.  
  - **Organizational unit**—Department within an organization.  
  - **State**—State of origin.  
  - **Country**—Country of origin. | detail          |
| Subject             | Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:  
  - **Common name**—Name of the authority.  
  - **Organization**—Organization of origin.  
  - **Organizational unit**—Department within an organization.  
  - **State**—State of origin.  
  - **Country**—Country of origin. | detail          |
| Alternate subject   | Domain name or IP address of the device related to the digital certificate.       | detail          |
| Validity            | Time period when the digital certificate is valid. Values are:  
  - **Not before**—Start time when the digital certificate becomes valid.  
  - **Not after**—End time when the digital certificate becomes invalid. | All levels      |
| Public key algorithm | Encryption algorithm used with the private key, such as **rsaEncryption** (1024 bits). | All levels      |
Table 104: show security pki local-certificate Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public key verification status</td>
<td>Public key verification status: Failed or Passed. The detail output also provides the verification hash.</td>
<td>All levels</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption.</td>
<td>detail</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Distribution CRL</td>
<td>Distinguished name information and URL for the certificate revocation list (CRL) server.</td>
<td>detail</td>
</tr>
<tr>
<td>Use for key</td>
<td>Use of the public key, such as Certificate signing, CRL signing, Digital signature, or Key encipherment.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

**show security pki local-certificate**

user@switch>  show security pki local-certificate

Certificate identifier: local-entrust2
  Issued to: router2.juniper.net, Issued by: juniper
  Validity:
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed

**show security pki local-certificate detail**

user@switch>  show security pki local-certificate detail

Certificate identifier: local-entrust3
  Certificate version: 3
  Serial number: 4355 94f9
  Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us, Common name: switch1.juniper.net
Alternate subject: switch1.juniper.net
Validity:
- Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```
```
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
```
```
Distribution CRL:
- C=us, O=juniper, CN=CRL1
  - http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
show security tpm status

Syntax

```
show security tpm status
```

Release Information

Command introduced in Junos OS Release 15.1X49-D80.
TPM Family and TPM Firmware version details are introduced in Junos OS Release 15.1X49-D120.

Description

Display the current status of the Trusted Platform Module (TPM). You can use this `show security tpm status` command to check the status of TPM ownership, master binding key, master encryption password, family version, and firmware version.

Options

This command has no options.

Required Privilege Level

security

RELATED DOCUMENTATION

- Using Trusted Platform Module to Bind Secrets on SRX Series Devices | 202
- `request security tpm master-encryption-password set` | 2517

List of Sample Output

show security tpm status on page 2782

Sample Output

```
show security tpm status

user@host> show security tpm status

TPM Status:
   Enabled: yes
   Owned: yes
   Master Binding Key: not-created
```
Table 105 on page 2783 lists the output fields for the **show security tpm status** command.

**Table 105: show security tpm status Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Specifies whether TPM is enabled or disabled.</td>
</tr>
<tr>
<td>Owned</td>
<td>Specifies the TPM ownership. TPM can be owned even if the Master Encryption Key and Master Encryption Key are not created/configured.</td>
</tr>
<tr>
<td>Master Binding Key</td>
<td>Displays the TPM’s Master Binding Key status whether it is created or not created. TPM generates cryptographic keys and encrypts them so that those can only be decrypted by the TPM. This process is know as binding. Each TPM has a master binding key, which is also know as storage root key.</td>
</tr>
<tr>
<td>Master Encryption Key</td>
<td>Displays Master Encryption Password status whether it is set or not set. The encrypted data and the hash of the configuration is protected by the TPM module using the master encryption password.</td>
</tr>
<tr>
<td>TPM Family</td>
<td>Displays Trusted Computing Group’s (TCG) TPM family version.</td>
</tr>
<tr>
<td>TPM Firmware version</td>
<td>Displays the firmware version loaded in TPM.</td>
</tr>
</tbody>
</table>
show services unified-access-control authentication-table

Syntax

```
show services unified-access-control authentication-table
```

Release Information


Description

Display a summary of the authentication table entries configured from the IC Series UAC Appliance. Authentication tables store mappings between traffic sessions and Unified Access Control (UAC) roles. The IC Series appliance uses the roles specified in the mappings to help determine which UAC policies to apply to a session.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a UAC deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC’s IC Series appliance.

You can also use this command to display the content of the authentication table in a user role firewall implementation. The table, pushed from a supporting UAC device, provides the user roles associated with incoming traffic.

Options

- **detail**—Display a detailed view of all authentication table entries.
- **extended**—Display a view of all authentication table entries with the user roles listed.
- **identifier id**—Display all authentication table entries with the specified identifier number.
- **ip source-ip-address**—Display any authentication table entry for the specified IP address.
- **role role-name**—Display all authentication table entries for the specified role name.
- **user username**—Display all authentication table entries for the specified user.

Required Privilege Level

view

RELATED DOCUMENTATION

- *Firewall User Authentication Overview*
Sample Output

show services unified-access-control authentication-table

user@host>show services unified-access-control authentication-table

<table>
<thead>
<tr>
<th>Id</th>
<th>Source IP</th>
<th>Username</th>
<th>Age</th>
<th>Role identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>198.51.100.22</td>
<td>user1</td>
<td>0</td>
<td>0000000001.000005.0</td>
</tr>
</tbody>
</table>

Total: 1

show services unified-access-control authentication-table detail

user@host>show services unified-access-control authentication-table detail

Identifier: 1
Source IP: 198.51.100.22
Username: john
Age: 0
Role identifier     Role name
0000000001.000005.0 Users
1113249951.100616.0 PersonalFirewall
1183670148.427197.0 UAC

Total: 1

show services unified-access-control authentication-table extended

user@host>show services unified-access-control authentication-table extended

<table>
<thead>
<tr>
<th>Id</th>
<th>Source IP</th>
<th>Username</th>
<th>Age</th>
<th>Role name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10.214.161.195</td>
<td>johna</td>
<td>60</td>
<td>Users, PersonalFirewall</td>
</tr>
<tr>
<td>6</td>
<td>10.214.161.183</td>
<td>mayb</td>
<td>60</td>
<td>role-1</td>
</tr>
</tbody>
</table>
show services unified-access-control authentication-table identifier id

user@host> show services unified-access-control authentication-table identifier 1

Identifier: 1
Source IP: 10.214.161.195
Username: johna
Age: 0
Role identifier       Role name
0000000001.000005.0 Users
1113249951.100616.0 PersonalFirewall
1183670148.427197.0 UAC
Total: 1

show services unified-access-control authentication-table ip

user@host> show services unified-access-control authentication-table ip 10.214.161.183

<table>
<thead>
<tr>
<th>Id</th>
<th>Source IP</th>
<th>Username</th>
<th>Age</th>
<th>Role identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>10.214.161.183</td>
<td>mayb</td>
<td>0</td>
<td>1420298444.225667.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total: 1</td>
</tr>
</tbody>
</table>

show services unified-access-control authentication-table role

user@host> show services unified-access-control authentication-table role role-1

<table>
<thead>
<tr>
<th>Id</th>
<th>Source IP</th>
<th>Username</th>
<th>Age</th>
<th>Role identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>10.214.161.183</td>
<td>maybe</td>
<td>60</td>
<td>1420298444.225667.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total: 1</td>
</tr>
</tbody>
</table>

show services unified-access-control authentication-table user username

user@host> show services unified-access-control authentication-table user prasanta

<table>
<thead>
<tr>
<th>Id</th>
<th>Source IP</th>
<th>Username</th>
<th>Age</th>
<th>Role identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>10.214.161.195</td>
<td>paul1</td>
<td>0</td>
<td>0000000001.000005.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total: 1</td>
</tr>
</tbody>
</table>
show services unified-access-control policies

Syntax

```
show services unified-access-control policies
```

Release Information

Command introduced in Junos OS Release 9.4.

Description

Display a summary of resource access policies configured from the IC Series UAC Appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

Options

- **detail**—Display a detailed view of all policies.
- **identifier id**—Display information about a specific policy by identification number.

Required Privilege Level

view

RELATED DOCUMENTATION

- *Firewall User Authentication Overview*

List of Sample Output

- show services unified-access-control policies on page 2787
- show services unified-access-control policies detail on page 2788
- show services unified-access-control policies identifier 1 on page 2788

Sample Output

```
show services unified-access-control policies

user@host> show services unified-access-control policies
```
<table>
<thead>
<tr>
<th>Id</th>
<th>Resource</th>
<th>Action</th>
<th>Apply</th>
<th>Role identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.100.15.0/24:*</td>
<td>allow</td>
<td>selected</td>
<td>1113249951.100616.0</td>
</tr>
<tr>
<td>2</td>
<td>10.100.17.0/24:*</td>
<td>deny</td>
<td>all</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Output**

```bash
user@host> show services unified-access-control policies detail

Identifier: 1
Resource: 10.100.15.0/24:*  
Resource: 10.100.16.23-10.100.16.60:*  
Action: allow  
Apply: selected  
Role identifier  
Role name  
1113249951.100616.0 Personal Firewall  
1112927873.881659.0 Antivirus  
1183670148.427197.0 UAC

Identifier: 2
Resource: 10.100.17.0/24:*  
Resource: 10.100.16.23-10.100.16.60:*  
Resource: 10.100.18.0/24:*  
Action: deny  
Apply: all
```

**Sample Output**

```bash
user@host> show services unified-access-control policies identifier 1

Identifier: 1
Resource: 10.100.15.0/24:*  
Resource: 10.100.16.23-10.100.16.60:*  
Action: allow  
Apply: selected  
Role identifier  
Role name  
1113249951.100616.0 Personal Firewall
```
<table>
<thead>
<tr>
<th>ID</th>
<th>Antivirus Type</th>
<th>UAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1112927873.881659.0</td>
<td>Antivirus</td>
<td>UAC</td>
</tr>
<tr>
<td>1183670148.427197.0</td>
<td></td>
<td>UAC</td>
</tr>
</tbody>
</table>
show services unified-access-control status

Syntax

`show services unified-access-control status`

Release Information
Command introduced in Junos OS Release 9.4.

Description
Display the status of the connection between the SRX Series device and the IC Series UAC Appliance as well as statistics to help debug connections to the IC Series appliance.

Use this command when you have configured the SRX Series device to act as a Junos OS Enforcer in a Unified Access Control (UAC) deployment. When deployed as a Junos OS Enforcer, the SRX Series device enforces the policies that are defined on the UAC's IC Series appliance.

Required Privilege Level
view

RELATED DOCUMENTATION

Firewall User Authentication Overview

List of Sample Output
show services unified-access-control status on page 2790

Sample Output

`show services unified-access-control status`

```
user@host> show services unified-access-control status

Host Address Port Interface State
dev106vm26 10.64.11.106 11123 ge-0/0/0.0 connected
dev107vm26 10.64.11.106 11123 ge-0/0/0.0 closed
```
show snmp

There are several commands that you can access in Junos OS operational mode to monitor SNMP information. Some of the commands are:

- **show snmp health-monitor**, which displays the health monitor log and alarm information.
- **show snmp mib**, which displays information from the MIBs, such as device and system information.
- **show snmp statistics**, which displays SNMP statistics such as the number of packets, silent drops, and invalid output values.
- **show snmp rmon**, which displays the RMON alarm, event, history, and log information.

The following example provides sample output from the **show snmp health-monitor** command:

```
user@switch> show snmp health-monitor
```

<table>
<thead>
<tr>
<th>Alarm Index</th>
<th>Variable description</th>
<th>Value</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>Health Monitor: root file system utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>jnxHrStoragePercentUsed.1</td>
<td>58</td>
<td>active</td>
</tr>
<tr>
<td>32769</td>
<td>Health Monitor: /config file system utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>jnxHrStoragePercentUsed.2</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td>32770</td>
<td>Health Monitor: RE 0 CPU utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>jnxOperatingCPU.9.1.0.0</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td>32773</td>
<td>Health Monitor: RE 0 Memory utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>jnxOperatingBuffer.9.1.0.0</td>
<td>35</td>
<td>active</td>
</tr>
<tr>
<td>32775</td>
<td>Health Monitor: jkernel daemon CPU utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Init daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Chassis daemon</td>
<td>50</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Firewall daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Interface daemon</td>
<td>5</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>SNMP daemon</td>
<td>11</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>MIB2 daemon</td>
<td>42</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following example provides sample output from the **show snmp mib** command:
user@switch> show snmp mib walk system

sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel
JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC builder@abc.example.net:
/volume/build/junos/11.1/production/20100926.0/obj-xlr/bsd/sys/compile/JUNIPER-xxxxx

Build date: 2010-09-26 06:00:10 U
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 24444184
sysContact.0  = J Smith
sysName.0     = Lab QFX3500
sysLocation.0 = Lab
sysServices.0 = 4

The following example provides sample output from the show snmp statistics command:

user@switch> show snmp statistics

SNMP statistics:
Input:
  Packets: 0, Bad versions: 0, Bad community names: 0,
  Bad community uses: 0, ASN parse errors: 0,
  Too bigs: 0, No such names: 0, Bad values: 0,
  Read onlys: 0, General errors: 0,
  Total request varbinds: 0, Total set varbinds: 0,
  Get requests: 0, Get nexts: 0, Set requests: 0,
  Get responses: 0, Traps: 0,
  Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
  Throttle drops: 0, Duplicate request drops: 0
Output:
  Packets: 0, Too bigs: 0, No such names: 0,
  Bad values: 0, General errors: 0,
  Get requests: 0, Get nexts: 0, Set requests: 0,
  Get responses: 0, Traps: 0
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp mib</td>
<td>2793</td>
</tr>
<tr>
<td>show snmp statistics</td>
<td>2794</td>
</tr>
</tbody>
</table>
**show snmp statistics**

**Syntax**

```
show snmp statistics <subagents>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Option `subagents` introduced in Junos OS Release 14.2.

**Description**

Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

**Options**

`subagents`—(Optional) Display the statistics of the protocol data unit (PDU), the number of SNMP requests and responses per subagent, and the SNMP statistics received from each subagent per logical system.

**Required Privilege Level**

`view`

**RELATED DOCUMENTATION**

| clear snmp statistics |

**List of Sample Output**

- show snmp statistics on page 2799
- show snmp statistics subagents on page 2799

**Output Fields**

Table 106 on page 2795 describes the output fields for the `show snmp statistics` command. Output fields are listed in the approximate order in which they appear.
Table 106: show snmp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>Information about received packets:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—(snmpInPkts) Total number of messages delivered to the SNMP entity from the transport service.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad versions</strong>—(snmpInBadVersions) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad community names</strong>—(snmpInBadCommunityNames) Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad community uses</strong>—(snmpInBadCommunityUses) Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ASN parse errors</strong>—(snmpInASNParseErrs) Total number of ASN.1 BER errors encountered by the SNMP entity when decoding received SNMP messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Too big</strong>—(snmpInTooBig) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <strong>tooBig</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No such names</strong>—(snmpInNoSuchNames) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <strong>noSuchName</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad values</strong>—(snmpInBadValues) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of <strong>badValue</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read only</strong>—(snmpInReadOnlys) Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of <strong>readOnly</strong>. Only incorrect implementations of SNMP generate this error.</td>
</tr>
</tbody>
</table>
Table 106: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General errors—(snmpInGenErrs)</td>
<td>Total number of SNMP PDUs delivered to the SNMP entity with an error status field of genErr.</td>
</tr>
<tr>
<td>Total requests varbinds—(snmpInTotalReqVars)</td>
<td>Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP GetRequest and GetNext PDUs.</td>
</tr>
<tr>
<td>Total set varbinds—(snmpInSetVars)</td>
<td>Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP SetRequest PDUs.</td>
</tr>
<tr>
<td>Get requests—(snmpInGetRequests)</td>
<td>Total number of SNMP GetRequest PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Get nexts—(snmpInGetNexts)</td>
<td>Total number of SNMP GetNext PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Set requests—(snmpInSetRequests)</td>
<td>Total number of SNMP SetRequest PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Get responses—(snmpInGetResponses)</td>
<td>Total number of SNMP GetResponse PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Traps—(snmpInTraps)</td>
<td>Total number of SNMP traps generated by the SNMP entity.</td>
</tr>
<tr>
<td>Silent drops—(snmpSilentDrops)</td>
<td>Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.</td>
</tr>
<tr>
<td>Proxy drops—(snmpProxyDrops)</td>
<td>Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned.</td>
</tr>
<tr>
<td>Commit pending drops</td>
<td>Number of SNMP packets for Set requests dropped because of a previous pending SNMP Set request on the committed configuration.</td>
</tr>
<tr>
<td>Throttle drops</td>
<td>Number of SNMP packets for any requests dropped reaching the throttle limit.</td>
</tr>
</tbody>
</table>
Table 106: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3 Input</td>
<td>Information about SNMP version 3 packets:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown security models</strong>—(snmpUnknownSecurityModels) Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid messages</strong>—(snmpInvalidMsgs) Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown pdu handlers</strong>—(snmpUnknownPDUHandlers) Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unavailable contexts</strong>—(snmpUnavailableContexts) Number of requests received for a context that is known to the SNMP engine, but is currently unavailable.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown contexts</strong>—(snmpUnknownContexts) Total number of requests received for a context that is unknown to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unsupported security levels</strong>—(usmStatsUnsupportedSecLevels) Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not in time windows</strong>—(usmStatsNotInTimeWindows) Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine’s window.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown user names</strong>—(usmStatsUnknownUserNames) Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown engine ids</strong>—(usmStatsUnknownEngineIDs) Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Wrong digests</strong>—(usmStatsWrongDigests) Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Decryption errors</strong>—(usmStatsDecryptionErrors) Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.</td>
</tr>
</tbody>
</table>
Table 106: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>Information about transmitted packets:</td>
</tr>
<tr>
<td></td>
<td>• Packets—(snmpOutPkts) Total number of messages passed from the SNMP entity to the transport service.</td>
</tr>
<tr>
<td></td>
<td>• Too bigs—(snmpOutTooBigs) Total number of SNMP PDUs generated by the SNMP entity with an error status field of tooBig.</td>
</tr>
<tr>
<td></td>
<td>• No such names—(snmpOutNoSuchNames) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of noSuchName.</td>
</tr>
<tr>
<td></td>
<td>• Bad values—(snmpOutBadValues) Total number of SNMP PDUs generated by the SNMP entity with an error status field of badValue.</td>
</tr>
<tr>
<td></td>
<td>• General errors—(snmpOutGenErrs) Total number of SNMP PDUs generated by the SNMP entity with an error status field of genErr.</td>
</tr>
<tr>
<td></td>
<td>• Get requests—(snmpOutGetRequests) Total number of SNMP GetRequest PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td></td>
<td>• Get nexts—(snmpOutGetNexts) Total number of SNMP GetNext PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td></td>
<td>• Set requests—(snmpOutSetRequests) Total number of SNMP SetRequest PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td></td>
<td>• Get responses—(snmpOutGetResponses) Total number of SNMP GetResponse PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td></td>
<td>• Traps—(snmpOutTraps) Total number of SNMP traps generated by the SNMP entity.</td>
</tr>
</tbody>
</table>

Table 107 on page 2798 describes the output fields for the `show snmp statistics subagents` command. Output fields are listed in the approximate order in which they appear.

Table 107: show snmp statistics subagents Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subagent</td>
<td>Location of the SNMP subagent.</td>
</tr>
<tr>
<td>Request PDUs</td>
<td>Number of PDUs requested by the SNMP manager.</td>
</tr>
<tr>
<td>Response PDUs</td>
<td>Number of response PDUs sent by the SNMP subagent.</td>
</tr>
<tr>
<td>Request Variables</td>
<td>Number of variable bindings on the PDUs requested by the SNMP manager.</td>
</tr>
<tr>
<td>Response Variables</td>
<td>Number of variable bindings on the PDUs sent by the SNMP subagent.</td>
</tr>
<tr>
<td>Average Response Time</td>
<td>Average time taken by the SNMP subagent to send statistics response.</td>
</tr>
</tbody>
</table>
### Table 107: show snmp statistics subagents Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Response Time</td>
<td>Maximum time taken by the SNMP subagent to send the statistics response.</td>
</tr>
</tbody>
</table>

### Sample Output

**show snmp statistics**

```
user@host> show snmp statistics

SNMP statistics:
Input:
   Packets: 246213, Bad versions: 12, Bad community names: 12,
   Bad community uses: 0, ASN parse errors: 96,
   Too bigs: 0, No such names: 0, Bad values: 0,
   Read onlys: 0, General errors: 0,
   Total request varbinds: 227084, Total set varbinds: 67,
   Get requests: 44942, Get nexts: 190371, Set requests: 10712,
   Get responses: 0, Traps: 0,
   Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
   Throttle drops: 0,
V3 Input:
   Unknown security models: 0, Invalid messages: 0
   Unknown pdu handlers: 0, Unavailable contexts: 0
   Unknown contexts: 0, Unsupported security levels: 1
   Not in time windows: 0, Unknown user names: 0
   Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0
Output:
   Packets: 246093, Too bigs: 0, No such names: 31561,
   Bad values: 0, General errors: 2,
   Get requests: 0, Get nexts: 0, Set requests: 0,
   Get responses: 246025, Traps: 0
```

**show snmp statistics subagents**

```
user@host> show snmp statistics subagents

Subagent: /var/run/cosd-20
   Request PDUs: 0, Response PDUs: 0,
   Request Variables: 0, Response Variables: 0,
```
Average Response Time(ms): 0.00,  
Maximum Response Time(ms): 0.00

Subagent: /var/run/pfed-30
  Request PDUs: 0, Response PDUs: 0,  
  Request Variables: 0, Response Variables: 0,  
  Average Response Time(ms): 0.00,  
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rmopd-15
  Request PDUs: 0, Response PDUs: 0,  
  Request Variables: 0, Response Variables: 0,  
  Average Response Time(ms): 0.00,  
  Maximum Response Time(ms): 0.00

Subagent: /var/run/chassisd-30
  Request PDUs: 33116, Response PDUs: 33116,  
  Request Variables: 33116, Response Variables: 33116,  
  Average Response Time(ms): 1.83,  
  Maximum Response Time(ms): 203.48

Subagent: /var/run/pkid-13
  Request PDUs: 0, Response PDUs: 0,  
  Request Variables: 0, Response Variables: 0,  
  Average Response Time(ms): 0.00,  
  Maximum Response Time(ms): 0.00

Subagent: /var/run/apsd-13
  Request PDUs: 0, Response PDUs: 0,  
  Request Variables: 0, Response Variables: 0,  
  Average Response Time(ms): 0.00,  
  Maximum Response Time(ms): 0.00

Subagent: /var/run/dfcd-32
  Request PDUs: 0, Response PDUs: 0,  
  Request Variables: 0, Response Variables: 0,  
  Average Response Time(ms): 0.00,  
  Maximum Response Time(ms): 0.00

Subagent: /var/run/mib2d-33
  Request PDUs: 74211, Response PDUs: 74211,  
  Request Variables: 74211, Response Variables: 74211,  
  Average Response Time(ms): 2.30,  
  Maximum Response Time(ms): 51.04
Subagent: /var/run/license-check-16
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/craftd-14
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/bfdd-19
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/smihelperd-24
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/cfmd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/rpd_snmp
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00

Subagent: /var/run/l2tpd-18
  Request PDUs: 0, Response PDUs: 0,
  Request Variables: 0, Response Variables: 0,
  Average Response Time(ms): 0.00,
  Maximum Response Time(ms): 0.00
show ssl-certificates

Syntax

```plaintext
show ssl certificates
```

Release Information

Command introduced in Junos OS Release 17.2R1 for EX Series switches.

Description

Display information about the Secure Sockets Layer (SSL) certificates installed on the switch. When you configure PEAP as the authentication protocol for MAC RADIUS authentication, you must load the server-side Secure Sockets Layer (SSL) certificate on the switch. PEAP requires an SSL certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. The key for this encryption are transported using the server’s public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

Options

- `none`—Display information about all SSL certificates.
- `detail`—Display information about SSL certificates for the specified level of output.

Required Privilege Level

`view`

RELATED DOCUMENTATION

- Configuring PEAP for MAC RADIUS Authentication

List of Sample Output

- show ssl-certificates on page 2803
- show ssl-certificates detail on page 2804

Output Fields

Table 104 on page 2779 lists the output fields for the `show ssl-certificates` command. Output fields are listed in the approximate order in which they appear.
### Table 108: show ssl-certificates Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• C—Country of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ST—State or province name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—Locality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• O—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OU—Organizational unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CN—Common name of the authority.</td>
<td></td>
</tr>
<tr>
<td>Valid from</td>
<td>Start time when the digital certificate becomes valid.</td>
<td>detail</td>
</tr>
<tr>
<td>Valid from</td>
<td>End time when the digital certificate becomes invalid.</td>
<td>detail</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Subject</td>
<td>Details of the digital certificate holder organized using the distinguished name format. Possible subfields are:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• C—Country of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ST—State or province name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—Locality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• O—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OU—Organizational unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CN—Common name of the authority.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

```plaintext
show ssl-certificates
user@root> show ssl-certificates

Issuer:
/C=IN/ST=KA/L=Blr/O=JNPRI/OU=CP/CN=User-RADIUS/emailAddress=user@juniper.net
```

show ssl-certificates detail

user@root> show ssl-certificates detail

Issuer:
/C=IN/ST=KA/L=Blr/O=JNPR/OU=CP/CN=User-Radius/emailAddress=user@juniper.net

Valid From:    May 30 17:41:04 2016 GMT
Valid Till:    May 29 17:41:04 2026 GMT
Serial Number: 0

Subject:
/C=IN/ST=KA/L=Blr/O=JNPR/OU=CP/CN=User-Radius/emailAddress=user@juniper.net
show subscribers

**Syntax**

```plaintext
show subscribers
<detail | extensive | terse>
<aci-interface-set-name aci-interface-set-name>
<address address>
<agent-circuit-identifier agent-circuit-identifier>
<agent-remote-identifier agent-remote-identifier>
<aggregation-interface-set-name interface-set-name>
<client-type client-type>
<count>
{id session-id <accounting-statistics>}
<interface interface <accounting-statistics>>
<logical-system logical-system>
<mac-address mac-address>
<physical-interface physical-interface-name>
<profile-name profile-name>
<routing-instance routing-instance>
<stacked-vlan-id stacked-vlan-id>
<subscriber-state subscriber-state>
<user-name user-name>
<vci vci-identifier>
<vpi vpi-identifier>
<vlan-id vlan-id>
```

**Release Information**

Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
**client-type**, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
**count** option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Enhanced subscriber management supported in Junos OS Release 15.1R3 on MX Series routers.
**accounting-statistics** option added in Junos OS Release 15.1R3 and 17.4R1 on MX Series routers.
**aggregation-interface-set-name** option added in Junos OS Release 18.4R1 on MX Series routers.
Description
Display information for active subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.0.2.0). If you specify the IP address as a prefix with a netmask (for example, 192.0.2.0/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified string. You can specify either the complete ACI string or a substring. To specify a substring, you must enter characters that form the beginning of the string, followed by an asterisk (*) as a wildcard to substitute for the remainder of the string. The wildcard can be used only at the end of the specified substring; for example:

user@host1> show subscribers agent-circuit-identifier substring*

<table>
<thead>
<tr>
<th>Junos OS Release</th>
<th>Substring Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos OS Release 13.3R1</td>
<td>You can specify a substring without a wildcard.</td>
</tr>
<tr>
<td>Starting in Junos OS Release 14.1R1</td>
<td>You must specify the complete ACI string; you cannot specify a wildcard.</td>
</tr>
<tr>
<td>Starting in Junos OS Release 15.1R7, 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, 17.4R2, 18.1R2, 18.2R1</td>
<td>You can specify a substring, but you must include the wildcard character at the end of the substring.</td>
</tr>
</tbody>
</table>

agent-remote-identifier—(Optional) Display all dynamic subscriber sessions whose ARI value matches the specified string. You must specify the complete ACI string; you cannot specify a wildcard.

aggregation-interface-set-name interface-set-name—(Optional) Display summary information for the specified aggregation node interface set, including interface, VLAN ID, username and LS:RI.

client-type—(Optional) Display subscribers whose client type matches one of the following client types:

- dhcp—DHCP clients only.
- dotlx—Dotlx clients only.
- **essm**—ESSM clients only.
- **fixed-wireless-access**—Fixed wireless access clients only.
- **fwauth**—FwAuth (authenticated across a firewall) clients only.
- **hag-bundle**—HAG tunnel bundle clients only.
- **hag-tunnel**—HAG tunnel clients only.
- **l2tp**—L2TP clients only.
- **mlppp**—MLPPP clients only.
- **ppp**—PPP clients only.
- **pppoe**—PPPoE clients only.
- **static**—Static clients only.
- **vlan**—VLAN clients only.
- **vlan-oob**—VLAN out-of-band (ANCP-triggered) clients only.
- **vpls-pw**—VPLS pseudowire clients only.
- **xauth**—Xauth clients only.

**count**—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the **count** option alone or with the **address**, **client-type**, **interface**, **logical-system**, **mac-address**, **profile-name**, **routing-instance**, **stacked-vlan-id**, **subscriber-state**, or **vlan-id** options.

**id session-id**—(Optional) Display a specific subscriber session whose session ID matches the specified subscriber ID. You can display subscriber IDs by using the **show subscribers extensive** or the **show subscribers interface extensive** commands.

**id session-id accounting-statistics**—(Optional) Display accurate subscriber accounting statistics for a subscriber session with the specified ID. Requires the **actual-transmit-statistics** statement to be configured in the dynamic profile for the dynamic logical interface. If the statement is not configured, a value of 0 is displayed for accounting statistics.

**interface**—(Optional) Display subscribers whose interface matches the specified interface.

**interface accounting-statistics**—(Optional) Display subscriber accounting statistics for the specified interface. Requires the **actual-transmit-statistics** statement to be configured in the dynamic profile for the dynamic logical interface.

**logical-system**—(Optional) Display subscribers whose logical system matches the specified logical system.

**mac-address**—(Optional) Display subscribers whose MAC address matches the specified MAC address.

**physical-interface-name**—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.
**profile-name**—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

**routing-instance**—(Optional) Display subscribers whose routing instance matches the specified routing instance.

**stacked-vlan-id**—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

**subscriber-state**—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

**user-name**—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

**vci-identifier**—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is 0 through 255.

**vpi-identifier**—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is 0 through 65,535.

**vlan-id**—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID, regardless of whether the subscriber uses a single-tagged or double-tagged VLAN. For subscribers using a double-tagged VLAN, this option displays subscribers where the inner VLAN tag matches the specified VLAN ID. To display only subscribers where the specified value matches only double-tagged VLANs, use the `stacked-vlan-id stacked-vlan-id` option to match the outer VLAN tag.

**NOTE:** Because of display limitations, logical system and routing instance output values are truncated when necessary.

**Required Privilege Level**

view

**RELATED DOCUMENTATION**

- **show subscribers summary**
- **Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration**
- **Verifying and Managing Configurations for Dynamic VLANS Based on Access-Line Identifiers**
- **Verifying and Managing Junos OS Enhanced Subscriber Management**
List of Sample Output

show subscribers (IPv4) on page 2820
show subscribers (IPv6) on page 2820
show subscribers (IPv4 and IPv6 Dual Stack) on page 2820
show subscribers (Single Session DHCP Dual Stack) on page 2821
show subscribers (Single Session DHCP Dual Stack detail) on page 2821
show subscribers (LNS on MX Series Routers) on page 2822
show subscribers (L2TP Switched Tunnels) on page 2822
show subscribers aggregation-interface-set-name on page 2822
show subscribers client-type dhcp detail on page 2822
show subscribers client-type dhcp detail (DHCPv6) on page 2823
show subscribers client-type dhcp extensive on page 2824
show subscribers client-type fixed-wireless-access on page 2825
show subscribers client-type fixed-wireless-access detail (Detail) on page 2825
show subscribers client-type hag-bundle on page 2826
show subscribers client-type hag-bundle (Detail) on page 2826
show subscribers client-type -hag-tunnel on page 2826
show subscribers client-type hag-tunnel (Detail) on page 2827
show subscribers client-type vlan-ooob detail on page 2827
show subscribers count on page 2828
show subscribers address detail (IPv6) on page 2828
show subscribers detail (IPv4) on page 2829
show subscribers detail (IPv6) on page 2829
show subscribers detail (pseudowire Interface for GRE Tunnel) on page 2830
show subscribers detail (IPv6 Static Demux Interface) on page 2830
show subscribers detail (L2TP LNS Subscribers on MX Series Routers) on page 2830
show subscribers detail (L2TP Switched Tunnels) on page 2831
show subscribers detail (Tunneled Subscriber) on page 2832
show subscribers detail (IPv4 and IPv6 Dual Stack) on page 2832
show subscribers detail (ACI Interface Set Session) on page 2833
show subscribers detail (PPPoE Subscriber Session with ACI Interface Set) on page 2834
show subscribers extensive on page 2834
show subscribers extensive (Aggregation Node Interface Set and DSL Forum Attributes) on page 2835
show subscribers extensive (Passive Optical Network Circuit Interface Set) on page 2836
show subscribers extensive (DNS Addresses from Access Profile or Global Configuration) on page 2837
show subscribers extensive (DNS Addresses from RADIUS) on page 2838
show subscribers extensive (IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration) on page 2838
show subscribers extensive (RPF Check Fail Filter) on page 2839
show subscribers extensive (L2TP LNS Subscribers on MX Series Routers) on page 2839
show subscribers extensive (IPv4 and IPv6 Dual Stack) on page 2840
show subscribers extensive (ADFRules) on page 2841
show subscribers extensive (Effective Shaping-Rate) on page 2842
show subscribers extensive (PPPoE Subscriber Access Line Rates on page 2842
show subscribers extensive (Subscriber Session Using PCEF Profile) on page 2844
show subscribers aci-interface-set-name detail ( Subscriber Sessions Using Specified ACI Interface Set) on page 2845
show subscribers agent-circuit-identifier detail ( Subscriber Sessions Using Specified ACI Substring) on page 2846
show subscribers id accounting-statistics on page 2847
show subscribers interface accounting-statistics on page 2847
show subscribers interface extensive on page 2848
show subscribers logical-system terse on page 2849
show subscribers physical-interface count on page 2849
show subscribers routing-instance inst1 count on page 2850
show subscribers stacked-vlan-id detail on page 2850
show subscribers stacked-vlan-id vlan-id detail (Combined Output) on page 2850
show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface) on page 2850
show subscribers user-name detail on page 2851
show subscribers vlan-id on page 2851
show subscribers vlan-id detail on page 2851
show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session) on page 2852
show subscribers address detail (Enhanced Subscriber Management) on page 2852

Output Fields
Table 109 on page 2810 lists the output fields for the show subscribers command. Output fields are listed in the approximate order in which they appear.

Table 109: show subscribers Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.</td>
</tr>
<tr>
<td>IP Address/VLAN ID</td>
<td>Subscriber IP address or VLAN ID associated with the subscriber in the form tpid.vlan-id No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is <strong>Tunnel-switched</strong>.</td>
</tr>
<tr>
<td>User Name</td>
<td>Name of subscriber.</td>
</tr>
<tr>
<td>LS:RI</td>
<td>Logical system and routing instance associated with the subscriber.</td>
</tr>
</tbody>
</table>
Table 109: show subscribers Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Subscriber client type (DHCP, FWA, GRE, HAG-BUNDLE, HAG-TUNNEL, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Subscriber IPv4 address.</td>
</tr>
<tr>
<td><strong>IP Netmask</strong></td>
<td>Subscriber IP netmask. (MX Series) This field displays 255.255.255.255 by default. For tunneled or terminated PPP subscribers only, this field displays the actual value of Framed-IP-Netmask when the SDB_FRAMED_PROTOCOL attribute in the session database is equal to AUTHD_FRAMED_PROTOCOL_PPP. This occurs in the use case where the LNS generates access-internal routes when it receives Framed-IP-Netmask from RADIUS during authorization. When it receives Framed-Pool from RADIUS, the pool mask is ignored and the default /32 mask is used.</td>
</tr>
<tr>
<td><strong>Primary DNS Address</strong></td>
<td>IP address of primary DNS server.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the address is provided by RADIUS.</td>
</tr>
<tr>
<td><strong>Secondary DNS Address</strong></td>
<td>IP address of secondary DNS server.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the address is provided by RADIUS.</td>
</tr>
<tr>
<td><strong>IPv6 Primary DNS Address</strong></td>
<td>IPv6 address of primary DNS server.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the address is provided by RADIUS.</td>
</tr>
<tr>
<td><strong>IPv6 Secondary DNS Address</strong></td>
<td>IPv6 address of secondary DNS server.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the address is provided by RADIUS.</td>
</tr>
<tr>
<td><strong>Domain name server inet</strong></td>
<td>IP addresses for the DNS server, displayed in order of configuration.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the addresses are derived from the access profile or the global access configuration.</td>
</tr>
<tr>
<td><strong>Domain name server inet6</strong></td>
<td>IPv6 addresses for the DNS server, displayed in order of configuration.</td>
</tr>
<tr>
<td></td>
<td>This field is displayed with the <em>extensive</em> option only when the addresses are derived from the access profile or the global access configuration.</td>
</tr>
<tr>
<td><strong>Primary WINS Address</strong></td>
<td>IP address of primary WINS server.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secondary WINS Address</strong></td>
<td>IP address of secondary WINS server.</td>
</tr>
<tr>
<td><strong>IPv6 Address</strong></td>
<td>Subscriber IPv6 address, or multiple addresses.</td>
</tr>
<tr>
<td><strong>IPv6 Prefix</strong></td>
<td>Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.</td>
</tr>
<tr>
<td><strong>IPv6 User Prefix</strong></td>
<td>IPv6 prefix obtained through NDRA.</td>
</tr>
<tr>
<td><strong>IPv6 Address Pool</strong></td>
<td>Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.</td>
</tr>
<tr>
<td><strong>IPv6 Network Prefix Length</strong></td>
<td>Length of the network portion of the IPv6 address.</td>
</tr>
<tr>
<td><strong>IPv6 Prefix Length</strong></td>
<td>Length of the subscriber IPv6 prefix.</td>
</tr>
<tr>
<td><strong>Logical System</strong></td>
<td>Logical system associated with the subscriber.</td>
</tr>
<tr>
<td><strong>Routing Instance</strong></td>
<td>Routing instance associated with the subscriber.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>(Enhanced subscriber management for MX Series routers) Name of the enhanced subscriber management logical interface, in the form demux0.nnnn (for example, demux0.3221225472), to which access-internal and framed subscriber routes are mapped.</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>Whether the subscriber interface is Static or Dynamic.</td>
</tr>
</tbody>
</table>
### Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Interface Set               | Internally generated name of the dynamic ACI or ALI interface set used by the subscriber session. The prefix of the name indicates the string received in DHCP or PPPoE control packets on which the interface set is based. For ALI interface sets, the prefix indicates that the value is configured as a trusted option to identify the subscriber line. The name of the interface set uses one of the following prefixes:  
  - aci—ACI; for example, aci-1033-demux0.3221225524. This is the only prefix allowed for ACI interface sets.  
  - ari—ARI; for example, ari-1033-demux0.3221225524.  
  - aci+ari—Both the ACI and ARI; for example, aci+ari-1033-demux0.3221225524.  
  - noids—Neither the ACI nor the ARI were received; for example, noids-1033-demux0.3221225524.  
  
  **NOTE:** ACI interface sets are configured with the `agent-circuit-identifier` autoconfiguration stanza. ALI interface sets are configured with the `line-identity` autoconfiguration stanza. Besides dynamic ACI and ALI interface sets, this field can be an interface set based on a substring of the ARI string. This occurs when the dynamic profile includes the predefined variable `$junos-pon-id-interface-set-name`, and the profile is applied for a passive optical network (PON). The ARI string is inserted by the optical line terminal (OLT). The final substring in the string, unique for the PON, identifies individual subscriber circuits, and is used as the name of the interface set. |
| Interface Set Type          | Interface type of the ACI interface set: **Dynamic**. This is the only ACI interface set type currently supported. |
| Interface Set Session ID    | Identifier of the dynamic ACI interface set entry in the session database. |
| Underlying Interface        | Name of the underlying interface for the subscriber session. |
| Dynamic Profile Name        | Dynamic profile used for the subscriber. For a HAG bundle, the profile that creates the bundle interface, which represents the subscriber interface. For a HAG tunnel, the profile the creates the DSL or LTE tunnel interface. |
| Dynamic Profile Version     | Version number of the dynamic profile used for the subscriber. |
| MAC Address                 | MAC address associated with the subscriber. |
| State                       | Current state of the subscriber session (**Init**, **Configured**, **Active**, **Terminating**, **Tunneled**) |
Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP State</td>
<td>Current state of the L2TP session, <strong>Tunneled</strong> or <strong>Tunnel-switched</strong>. When the value is <strong>Tunnel-switched</strong>, two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.</td>
</tr>
<tr>
<td>Tunnel switch Profile Name</td>
<td>Name of the L2TP tunnel switch profile that initiates tunnel switching.</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>IP address of the local gateway (LAC).</td>
</tr>
<tr>
<td>Remote IP Address</td>
<td>IP address of the remote peer (LNS).</td>
</tr>
<tr>
<td>PFE Flow ID</td>
<td>Forwarding flow identifier.</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>VLAN ID associated with the subscriber in the form <code>tpid.vlan-id</code>.</td>
</tr>
<tr>
<td>Stacked VLAN Id</td>
<td>Stacked VLAN ID associated with the subscriber in the form <code>tpid.vlan-id</code>.</td>
</tr>
<tr>
<td>RADIUS Accounting ID</td>
<td>RADIUS accounting ID associated with the subscriber.</td>
</tr>
<tr>
<td>Agent Circuit ID</td>
<td>For the <strong>dhcp</strong> client type, option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.</td>
</tr>
<tr>
<td></td>
<td>For the <strong>vlan-oob</strong> client type, the agent circuit ID or access-loop circuit identifier that identifies the subscriber line based on the subscriber-facing DSLAM interface on which the subscriber request originates.</td>
</tr>
<tr>
<td>Agent Remote ID</td>
<td>For the <strong>dhcp</strong> client type, option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.</td>
</tr>
<tr>
<td></td>
<td>For the <strong>vlan-oob</strong> client type, the agent remote ID or access-loop remote identifier that identifies the subscriber line based on the NAS-facing DSLAM interface on which the subscriber request originates.</td>
</tr>
</tbody>
</table>
Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Aggregation Interface-set Name** | Value of the $junos-aggregation-interface-set-name predefined variable; one of the following:  
  - When the **hierarchical-access-network-detection** option is configured for the access lines and the value of the Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x0003) received either in the ANCP Port Up message or PPPoE PADR IA tags begins with a # character, then the variable takes the value of the remainder of the string after the # character.  
  - When the **hierarchical-access-network-detection** option is not configured, or if the string does not begin with the # character, then the variable takes the value specified with the **predefined-variable-defaults** statement. |
| **Accounting Statistics**       | Actual transmitted subscriber accounting statistics by session ID or interface. Service accounting statistics are not included. These statistics do not include overhead bytes or dropped packets; they are the accurate statistics used by RADIUS. The statistics are counted when the **actual-transmit-statistics** statement is included in the dynamic profile. |
| **DHCP Relay IP Address**       | IP address used by the DHCP relay agent.                                                                                                                                                                         |
| **ATM VPI**                     | (MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber’s physical interface.                                                                             |
| **ATM VCI**                     | (MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.                                                            |
| **Login Time**                  | Date and time at which the subscriber logged in.                                                                                                                                                                 |
| **DHCPV6 Options**              | len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.                                                                                             |
| **Server DHCP Options**         | len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options.                                                                                            |
| **Server DHCPV6 Options**       | len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.                                                                                           |
| **DHCPV6 Header**               | len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCPv6 options.                                                                                           |
| **Effective shaping-rate**      | Actual downstream traffic shaping rate for the subscriber, in kilobits per second.                                                                                                                                |
Table 109: show subscribers Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Input Service Set</td>
<td>Input service set in access dynamic profile.</td>
</tr>
<tr>
<td>IPv4 Output Service Set</td>
<td>Output service set in access dynamic profile.</td>
</tr>
<tr>
<td>PCEF Profile</td>
<td>PCEF profile in access dynamic profile.</td>
</tr>
<tr>
<td>PCEF Rule/Rulebase</td>
<td>PCC rule or rulebase used in dynamic profile.</td>
</tr>
<tr>
<td>Dynamic configuration</td>
<td>Values for variables that are passed into the dynamic profile from RADIUS.</td>
</tr>
<tr>
<td>Service activation time</td>
<td>Time at which the first family in this service became active.</td>
</tr>
<tr>
<td>IPv4 rpf-check Fail Filter Name</td>
<td>Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.</td>
</tr>
<tr>
<td>IPv6 rpf-check Fail Filter Name</td>
<td>Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.</td>
</tr>
<tr>
<td>Session ID</td>
<td>ID number for a subscriber session.</td>
</tr>
<tr>
<td>Underlying Session ID</td>
<td>For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.</td>
</tr>
<tr>
<td>Service Sessions</td>
<td>Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.</td>
</tr>
<tr>
<td>Service Session ID</td>
<td>ID number for a subscriber service session.</td>
</tr>
<tr>
<td>Service Session Name</td>
<td>Service session profile name.</td>
</tr>
<tr>
<td>Session Timeout (seconds)</td>
<td>Number of seconds of access provided to the subscriber before the session is automatically terminated.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Idle Timeout (seconds)</td>
<td>Number of seconds subscriber can be idle before the session is automatically terminated.</td>
</tr>
<tr>
<td>IPv6 Delegated Address Pool</td>
<td>Name of the pool used for DHCPv6 prefix delegation.</td>
</tr>
<tr>
<td>IPv6 Delegated Network Prefix Length</td>
<td>Length of the prefix configured for the IPv6 delegated address pool.</td>
</tr>
<tr>
<td>IPv6 Interface Address</td>
<td>Address assigned by the Framed-Ipv6-Prefix AAA attribute. This field is displayed only when the predefined variable $junos-ipv6-address is used in the dynamic profile.</td>
</tr>
<tr>
<td>IPv6 Framed Interface Id</td>
<td>Interface ID assigned by the Framed-Interface-Id AAA attribute.</td>
</tr>
<tr>
<td>ADF IPv4 Input Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>ADF IPv4 Output Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>ADF IPv6 Input Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>ADF IPv6 Output Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>IPv4 Input Filter Name</td>
<td>Name assigned to the IPv4 input filter (client or service session).</td>
</tr>
<tr>
<td>IPv4 Output Filter Name</td>
<td>Name assigned to the IPv4 output filter (client or service session).</td>
</tr>
<tr>
<td>IPv6 Input Filter Name</td>
<td>Name assigned to the IPv6 input filter (client or service session).</td>
</tr>
</tbody>
</table>
Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Output Filter Name</td>
<td>Name assigned to the IPv6 output filter (client or service session).</td>
</tr>
<tr>
<td>IFL Input Filter Name</td>
<td>Name assigned to the logical interface input filter (client or service session).</td>
</tr>
<tr>
<td>IFL Output Filter Name</td>
<td>Name assigned to the logical interface output filter (client or service session).</td>
</tr>
<tr>
<td>DSL type</td>
<td>PPPoE subscriber’s access line type reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute DSL-Type (0x0091). The DSL type is one of the following types: ADSL, ADSL2, ADSL2+, OTHER, SDSL, VDSL, or VDSL2.</td>
</tr>
</tbody>
</table>
| Frame/Cell Mode             | Mode type of the PPPoE subscriber’s access line determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091):  
- **Cell**—When the DSL line type is one of the following: ADSL, ADSL2, or ADSL2+.  
- **Frame**—When the DSL line type is one of the following: OTHER, SDSL, VDSL, or VDSL2.  
The value is stored in the subscriber session database. |
<p>| Overhead accounting bytes   | Number of bytes added to or subtracted from the actual downstream cell or frame overhead to account for the technology overhead of the DSL line type. The value is determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091). The value is stored in the subscriber session database. |
| Actual upstream data rate   | Unadjusted upstream data rate for the PPPoE subscriber’s access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Upstream (0x0081). |
| Actual downstream data rate | Unadjusted downstream data rate for the PPPoE subscriber’s access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Downstream (0x0082). |
| Adjusted downstream data rate | Adjusted downstream data rate for the PPPoE subscriber’s access line, calculated by the PPPoE daemon and stored in the subscriber session database. |
| Adjusted upstream data rate  | Adjusted upstream data rate for the PPPoE subscriber’s access line, calculated by the PPPoE daemon and stored in the subscriber session database. |</p>
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local TEID-U</td>
<td>Tunnel endpoint identifier on the BNG for the GTP-U user plane tunnel to the eNodeB. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the <strong>GTPU Tunnel Local IP address</strong> value.</td>
</tr>
<tr>
<td>Local TEID-C</td>
<td>Tunnel endpoint identifier on the BNG for the GTP-C control plane tunnel to the MME. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the <strong>GTPC Local IP address</strong> value.</td>
</tr>
<tr>
<td>Remote TEID-U</td>
<td>Tunnel endpoint identifier on the eNodeB for the GTP-U user plane tunnel to the BNG. The identifier is allocated by the eNodeB. A fully qualified remote TEID-U consists of this identifier and the <strong>GTPU Tunnel Remote IP address</strong> value.</td>
</tr>
<tr>
<td>Remote TEID-C</td>
<td>Tunnel endpoint identifier on the MME for the GTP-C control plane tunnel to the BNG. The identifier is allocated by the MME. A fully qualified remote TEID-C consists of this identifier and the <strong>GTPC Remote IP address</strong> value.</td>
</tr>
<tr>
<td>GTPU Tunnel Remote IP address</td>
<td>IP address of the S1-U interface on the eNodeB for the GTP-U tunnel endpoint. A fully qualified remote TEID-U consists of this address and the <strong>Remote TEID-U</strong> value.</td>
</tr>
<tr>
<td>GTPU Tunnel Local IP address</td>
<td>IP address of the S1-U interface on the BNG for the GTP-U tunnel endpoint. A fully qualified local TEID-U consists of this address and the <strong>Local TEID-U</strong> value.</td>
</tr>
<tr>
<td>GTPC Remote IP address</td>
<td>IP address of the S11 interface on the MME for the GTP-C tunnel endpoint. A fully qualified remote TEID-C consists of this address and the <strong>Remote TEID-C</strong> value.</td>
</tr>
<tr>
<td>GTPC Local IP address</td>
<td>IP address of the S11 interface on the BNG for the GTP-C tunnel endpoint. A fully qualified local TEID-C consists of this address and the <strong>Local TEID-C</strong> value.</td>
</tr>
<tr>
<td>Access Point Name</td>
<td>Access point name (APN) for the user equipment. The APN corresponds to the connection and service parameters that the subscriber’s mobile device can use for connecting to the carrier’s gateway to the Internet.</td>
</tr>
</tbody>
</table>
Table 109: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAG Session ID</td>
<td>ID number for the hybrid access gateway session. Sharing this ID bonds the DSL and LTE tunnels that make up the bundle.</td>
</tr>
<tr>
<td>HAG Tunnel Type</td>
<td>Type of HAG tunnel, DSL or LTE.</td>
</tr>
</tbody>
</table>

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
```

```
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     10                                    default:default
demux0.1073741824       203.0.113.10        WHOLESALER-CLIENT default:default
demux0.1073741825       203.0.113.3         RETAILER1-CLIENT test1:retailer1
demux0.1073741826       203.0.113.3         RETAILER2-CLIENT test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
```

```
Interface               IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001:db8:c0:0:0:0:0/74    WHOLESALER-CLIENT   default:default
*             2001:db8:1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
```

```
Interface           IP Address/VLAN ID         User Name                      LS:RI
demux0.1073741834   0x8100.1002 0x8100.1          default:default
default:default
demux0.1073741835   0x8100.1001 0x8100.1          default:default
default:default
pp0.1073741836      203.0.113.13             dualstackuser1@example1.com
default:ASP-1
*                   2001:db8:1::/48
*                   2001:db8:1:1::/64
```
show subscribers (Single Session DHCP Dual Stack)
user@host> show subscribers

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
<th>LS:RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>demux0.1073741364</td>
<td>192.168.10.10</td>
<td>dual-stack-retail35</td>
<td>default:default</td>
</tr>
<tr>
<td>default:default</td>
<td>2001:db8::100:0:0:0/74</td>
<td></td>
<td>default:default</td>
</tr>
<tr>
<td>default:default</td>
<td>2001:db8:3ffe:0:4::/64</td>
<td></td>
<td>default:default</td>
</tr>
</tbody>
</table>

show subscribers (Single Session DHCP Dual Stack detail)
user@host> show subscribers id 27 detail

Type: DHCP
User Name: dual-stack-retail33
IP Address: 10.10.0.53
IPv6 Address: 2001:db8:3000:0:0:8003::2
IPv6 Prefix: 2001:db8:3ffe:0:4::/64
Logical System: default
Routing Instance: default
Interface: ae0.3221225472
Interface type: Static
Underlying Interface: ae0.3221225472
Dynamic Profile Name: dhcp-retail-18
MAC Address: 00:00:5E:00:53:02
State: Active
DHCP Relay IP Address: 10.10.0.1
Radius Accounting ID: 27
Session ID: 27
PFE Flow ID: 2
Stacked VLAN Id: 2000
VLAN Id: 1
Login Time: 2014-05-15 10:12:10 PDT
DHCP Options: len 60
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 00 64 01 01 02
show subscribers (LNS on MX Series Routers)

user@host> show subscribers

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
<th>LS:RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>si-4/0/0.1</td>
<td>192.0.2.0</td>
<td><a href="mailto:user@example.com">user@example.com</a></td>
<td>default:default</td>
</tr>
</tbody>
</table>

show subscribers (L2TP Switched Tunnels)

user@host> show subscribers

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
<th>LS:RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>si-2/1/0.1073741842</td>
<td>Tunnel-switched</td>
<td><a href="mailto:user@example.com">user@example.com</a></td>
<td>default:default</td>
</tr>
<tr>
<td>si-2/1/0.1073741843</td>
<td>Tunnel-switched</td>
<td><a href="mailto:user@example.com">user@example.com</a></td>
<td>default:default</td>
</tr>
</tbody>
</table>

show subscribers aggregation-interface-set-name

user@host> show subscribers aggregation-interface-set-name FRA*

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/0.3221225472</td>
<td>50</td>
<td>ancp</td>
</tr>
<tr>
<td></td>
<td>default:isp1-subscriber</td>
<td></td>
</tr>
</tbody>
</table>

show subscribers client-type dhcp detail

user@host> show subscribers client-type dhcp detail

Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: user:2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 203.0.113.27
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:f3
State: Active
Radius Accounting ID: 1234:2560
Login Time: 2009-08-25 14:43:56 PDT

show subscribers client-type dhcp detail (DHCPv6)
user@host> show subscribers client-type dhcp detail

Type: DHCP
User Name: DEFAULTUSER
IPv6 Address: 2001:db8::2
IPv6 Prefix: 2001:db8:1::/64
Logical System: default
Routing Instance: default
Interface: demux0.3221225602
Interface type: Static
Underlying Interface: demux0.3221225602
Dynamic Profile Name: client-profile
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 142
Session ID: 142
PFE Flow ID: 148
Stacked VLAN Id: 1
VLAN Id: 1
Login Time: 2018-03-29 12:27:38 EDT
DHCP Options: len 56
00 08 00 02 00 00 00 01 00 0e 00 01 00 01 22 4f d0 33 00 11
show subscribers client-type dhcp extensive

user@host> show subscribers client-type dhcp extensive

Type: DHCP
User Name: user
IP Address: 192.0.2.4
IP Netmask: 255.0.0.0
IPv6 Address: 2001:db8:3::103
IPv6 Prefix: 2001:db8::/68
Domain name server inet6: 2001:db8:1 abcd::2
Logical System: default
Routing Instance: default
Interface: ge-0/0/0.0
Interface type: Static
Underlying Interface: ge-0/0/0.0
MAC Address: 00:00:5e:00:53:01
State: Configured
Radius Accounting ID: 10
Session ID: 10
PFE Flow ID: 2
VLAN Id: 100
Agent Circuit ID: ge-0/0/0:100
Agent Remote ID: ge-0/0/0:100
Login Time: 2017-05-23 12:52:22 IST
DHCPV6 Options: len 69
Server DHCP Options: len 13
Server DHCPV6 Options: len 8
show subscribers client-type fixed-wireless-access

user@host> show subscribers client-type fixed-wireless-access

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS:RI</td>
<td>192.0.2.10</td>
<td>505024101215074</td>
</tr>
<tr>
<td>ps1.3221225472</td>
<td>192.0.2.10</td>
<td>505024101215075</td>
</tr>
<tr>
<td>default:default</td>
<td>192.0.2.11</td>
<td></td>
</tr>
<tr>
<td>default:default</td>
<td>192.0.2.11</td>
<td></td>
</tr>
</tbody>
</table>

show subscribers client-type fixed-wireless-access detail (Detail)

user@host> show subscribers client-type fixed-wireless-access detail

**Type:** FWA

User Name: 505024101215074
IP Address: 192.0.2.10
IP Netmask: 255.255.0.0
Interface: ps1.3221225472
Interface type: Dynamic
Dynamic Profile Name: fwa-profile
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 11
Login Time: 2019-04-10 14:10:12 PDT
Local TEID-U: 1
Local TEID-C: 1
Remote TEID-U: 2000000
Remote TEID-C: 1000000
GTPU Tunnel Remote IP Address: 203.0.113.1.3
GTPU Tunnel Local IP Address: 203.0.113.2.5
GTPC Remote IP Address: 203.0.113.1.2
show subscribers client-type hag-bundle

user@host> show subscribers client-type hag-bundle

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS:RI</td>
<td>ps0.3221225473</td>
<td>user1</td>
</tr>
<tr>
<td></td>
<td>default:default</td>
<td></td>
</tr>
</tbody>
</table>

show subscribers client-type hag-bundle (Detail)

user@host> show subscribers client-type hag-bundle detail

Type: HAG-BUNDLE
User Name: user1
Logical System: default
Routing Instance: default
Interface: ps0.3221225473
Interface type: Dynamic
Dynamic Profile Name: hag-dyn-profile
State: Active
Radius Accounting ID: 2
Session ID: 2
HAG Session ID: 1634170802
PFE Flow ID: 9
Login Time: 2019-08-13 16:36:02 EDT

show subscribers client-type -hag-tunnel

user@host> show subscribers client-type hag-tunnel

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS:RI</td>
<td>ps0.3221225472</td>
<td>user1</td>
</tr>
<tr>
<td></td>
<td>default:default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ps0.3221225473</td>
<td>user1</td>
</tr>
<tr>
<td></td>
<td>default:default</td>
<td></td>
</tr>
</tbody>
</table>
show subscribers client-type hag-tunnel (Detail)

user@host> show subscribers client-type hag-tunnel detail

<table>
<thead>
<tr>
<th>Type: HAG-TUNNEL</th>
<th>User Name: user1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical System: default</td>
<td></td>
</tr>
<tr>
<td>Routing Instance: default</td>
<td></td>
</tr>
<tr>
<td>Interface: ps0.3221225472</td>
<td></td>
</tr>
<tr>
<td>Interface type: Dynamic</td>
<td></td>
</tr>
<tr>
<td>Dynamic Profile Name: hag-access-line-profile</td>
<td></td>
</tr>
<tr>
<td>State: Active</td>
<td></td>
</tr>
<tr>
<td>Session ID: 1</td>
<td></td>
</tr>
<tr>
<td>Bundle Session ID: 2</td>
<td></td>
</tr>
<tr>
<td>HAG Session ID: 1634170802</td>
<td></td>
</tr>
<tr>
<td>HAG Tunnel Type: LTE</td>
<td></td>
</tr>
<tr>
<td>PFE Flow ID: 7</td>
<td></td>
</tr>
<tr>
<td>Login Time: 2019-08-13 16:36:02 EDT</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type: HAG-TUNNEL</th>
<th>User Name: user1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical System: default</td>
<td></td>
</tr>
<tr>
<td>Routing Instance: default</td>
<td></td>
</tr>
<tr>
<td>Interface: ps0.3221225474</td>
<td></td>
</tr>
<tr>
<td>Interface type: Dynamic</td>
<td></td>
</tr>
<tr>
<td>Dynamic Profile Name: hag-access-line-profile</td>
<td></td>
</tr>
<tr>
<td>State: Active</td>
<td></td>
</tr>
<tr>
<td>Session ID: 3</td>
<td></td>
</tr>
<tr>
<td>Bundle Session ID: 2</td>
<td></td>
</tr>
<tr>
<td>HAG Session ID: 1634170802</td>
<td></td>
</tr>
<tr>
<td>HAG Tunnel Type: DSL</td>
<td></td>
</tr>
<tr>
<td>PFE Flow ID: 10</td>
<td></td>
</tr>
<tr>
<td>Login Time: 2019-08-13 16:36:02 EDT</td>
<td></td>
</tr>
</tbody>
</table>

show subscribers client-type vlan-oob detail

user@host> show subscribers client-type vlan-oob detail

<table>
<thead>
<tr>
<th>Type: VLAN-OOB</th>
<th>User Name: L2WS.line-aci-1.line-ari-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical System: default</td>
<td></td>
</tr>
<tr>
<td>Routing Instance: ISP1</td>
<td></td>
</tr>
<tr>
<td>Interface: demux0.1073744127</td>
<td></td>
</tr>
<tr>
<td>Interface type: Dynamic</td>
<td></td>
</tr>
<tr>
<td>Underlying Interface: ge-1/0/0</td>
<td></td>
</tr>
</tbody>
</table>
show subscribers count

user@host> show subscribers count

Total Subscribers: 188, Active Subscribers: 188

show subscribers address detail (IPv6)

user@host> show subscribers address 203.0.113.137 detail

Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 203.0.113.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 2001:db8:0:c88::/32
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:00:5e:00:53:53
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: example demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
show subscribers detail (IPv4)

user@host> show subscribers detail

Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Primary DNS Address: 192.0.2.0
Secondary DNS Address: 192.0.2.1
Primary WINS Address: 192.0.2.3
Secondary WINS Address: 192.0.2.4
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: example:2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 33 2d
37 2d 30 37 05 01 06 21 2c
Service Sessions: 2

show subscribers detail (IPv6)

user@host> show subscribers detail

Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:ffff:1::/32
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00
00 00

show subscribers detail (pseudowire Interface for GRE Tunnel)
user@host> show subscribers detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
<th>LS:RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>ps0.3221225484</td>
<td>192.0.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ps0.3221225485</td>
<td>192.0.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>demux0.3221225486</td>
<td>1</td>
<td></td>
<td>default:default</td>
</tr>
<tr>
<td>demux0.3221225487</td>
<td>1</td>
<td></td>
<td>default:default</td>
</tr>
<tr>
<td>demux0.3221225488</td>
<td>198.51.0.1</td>
<td></td>
<td>default:default</td>
</tr>
<tr>
<td>demux0.3221225489</td>
<td>198.51.0.2</td>
<td></td>
<td>default:default</td>
</tr>
</tbody>
</table>

show subscribers detail (IPv6 Static Demux Interface)
user@host> show subscribers detail

Type: STATIC-INTERFACE
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)
user@host> show subscribers detail
Type: L2TP
User Name: user@example.com
IP Address: 203.0.113.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-1ns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001

show subscribers detail (L2TP Switched Tunnels)

user@host> show subscribers detail

Type: L2TP
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.51
Remote IP Address: 192.0.2.0
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.31
Remote IP Address: 192.0.2.1
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST

show subscribers detail (Tunneled Subscriber)
user@host> show subscribers detail

Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512

show subscribers detail (IPv4 and IPv6 Dual Stack)
user@host> show subscribers detail

Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@example1.com
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00 00
00 00

show subscribers detail (ACI Interface Set Session)
user@host> show subscribers detail

Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
**Interface Set: aci-1001-ge-1/0/0.2800**
**Interface Set Session ID: 0**
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

user@host> show subscribers detail

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.15
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST

show subscribers extensive

user@host> show subscribers extensive

Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:ffff:1::/32
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48

show subscribers extensive (Aggregation Node Interface Set and DSL Forum Attributes)

user@host> show subscribers extensive

Type: VLAN-OOB
User Name: ancp
Logical System: default
Routing Instance: isp1-subscriber
Interface: ge-1/0/0.3221225472
Interface type: Dynamic
Interface Set: FRA-DPU-C-100
Underlying Interface: ge-1/0/0
Core IFL Name: ge-1/0/4.0
Dynamic Profile Name: Prof_L2BSA
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 13
VLAN Id: 50
VLAN Map Id: 20
Inner VLAN Map Id: 1
Inner VLAN Tag Protocol Id: 0x88a8
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id

Aggregation Interface-set Name: FRA-DPU-C-100
Login Time: 2018-05-29 08:43:42 EDT
Accounting interval: 72000
Dynamic configuration:
   junos-cos-scheduler-map: 100m
   junos-inner-vlan-tag-protocol-id: 0x88a8
   junos-vlan-map-id: 20

Type: PPPoE
IP Address: 192.85.128.1
IP Netmask: 255.255.255.255
Logical System: default
Routing Instance: default
Interface: pp0.3221225474
Interface type: Dynamic
Interface Set: ge-1/0/0
Underlying Interface: demux0.3221225473
Dynamic Profile Name: pppoe-client-profile-with-cos
MAC Address: 00:10:94:00:00:03
State: Active
Radius Accounting ID: 3
Session ID: 3
PFE Flow ID: 16
Stacked VLAN Id: 50
VLAN Id: 7
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id

**Aggregation Interface-set Name: FRA-DPU-C-100**
Login Time: 2018-05-29 08:43:45 EDT
IP Address Pool: pool-1
Accounting interval: 72000
DSL type: G.fast
Frame/cell mode: Frame
Overhead accounting bytes: 10
Actual upstream data rate: 100000 kbps
Actual downstream data rate: 200000 kbps
Calculated downstream data rate: 180000 kbps
Calculated upstream data rate: 90000 kbps
Adjusted upstream data rate: 80000 kbps
Adjusted downstream data rate: 160000 kbps

**DSL Line Attributes**
  - Agent Circuit ID: circuit 201
  - Agent Remote ID: remote-id
  - Actual upstream data rate: 100000
  - Actual downstream data rate: 200000
  - DSL type: G.fast
  - Access Aggregation Circuit ID: #FRA-DPU-C-100
  - Attribute type: 0xAA, Attribute length: 4
    198 51 100 78

show subscribers extensive (Passive Optical Network Circuit Interface Set)
user@host> show subscribers client-type dhcp extensive

Type: DHCP
IP Address: 192.0.2.136
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073741842
Interface type: Dynamic
show subscribers extensive (DNS Addresses from Access Profile or Global Configuration)

user@host> show subscribers extensive

Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Domain name server inet: 198.51.100.1 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
2837
show subscribers extensive (DNS Addresses from RADIUS)

user@host> show subscribers extensive

Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
**Primary DNS Address: 198.51.100.1**
**Secondary DNS Address: 198.51.100.2**
IPv6 Address: 2001:db8::1:11
**IPv6 Primary DNS Address: 2001:db8:5001::12**
**IPv6 Secondary DNS Address: 2001:db8:3001::12**
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00 00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 2f 2f 35 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool

show subscribers extensive (IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration)

user@host> show subscribers extensive

Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
**Primary DNS Address: 198.51.100.1**
**Secondary DNS Address: 198.51.100.2**
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 03 33 04 00 00 00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f 31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool

show subscribers extensive (RPF Check Fail Filter)
user@host> show subscribers extensive

...  
Type: VLAN  
  Logical System: default  
  Routing Instance: default  
  Interface: ae0.1073741824  
  Interface type: Dynamic  
  Dynamic Profile Name: vlan-prof  
  State: Active  
  Session ID: 9  
  VLAN Id: 100  
  Login Time: 2011-08-26 08:17:00 PDT  
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp  
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6  
...

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)
user@host> show subscribers extensive

Type: L2TP  
User Name: user@example.com
show subscribers extensive (IPv4 and IPv6 Dual Stack)

user@host> show subscribers extensive

Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@example1.com
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2001:db8:2016:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48

show subscribers extensive (ADF Rules)
user@host> show subscribers extensive

...
show subscribers extensive (Effective Shaping-Rate)

user@host> show subscribers extensive

Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
Effective shaping-rate: 31000000k
...

show subscribers extensive (PPPoE Subscriber Access Line Rates)

user@host> show subscribers extensive

Type: PPPoE
IP Address: 198.51.100.1
IP Netmask: 255.255.255.255
Logical System: default
Routing Instance: default
Interface: pp0.3221225475
Interface type: Dynamic
Underlying Interface: demux0.3221225474
Dynamic Profile Name: pppoe-client-profile-with-cos
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 4
Session ID: 4
PFE Flow ID: 14
Stacked VLAN Id: 40
VLAN Id: 1
Agent Circuit ID: circuit0
Agent Remote ID: remote0
Login Time: 2017-04-06 15:52:32 PDT

User Name: DAVE-L2BSA-SERVICE
Logical System: default
Routing Instance: isp-1-subscriber
Interface: ge-1/2/4.3221225472
Interface type: Dynamic
Interface Set: ge-1/2/4
Underlying Interface: ge-1/2/4
Core IFL Name: ge-1/3/4.0
Dynamic Profile Name: L2BSA-88a8-400LL1300VO
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 14
VLAN Id: 13
VLAN Map Id: 102
Inner VLAN Map Id: 1
Agent Circuit ID: circuit-aci-3
Agent Remote ID: remote49-3
Login Time: 2017-04-05 16:59:29 EDT
Service Sessions: 4
IFL Input Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-in
IFL Output Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-out
Accounting interval: 900
DSL type: VDSL
Frame/Cell Mode: Frame
Overhead accounting bytes: -10
Actual upstream data rate: 1024 kbps
Actual downstream data rate: 4096 kbps
Adjusted downstream data rate: 3686 kbps
Adjusted upstream data rate: 922 kbps
Dynamic configuration:
    junos-vlan-map-id: 102
    Service Session ID: 5
    Service Session Name: SRL-L1
    State: Active
    Family: inet, inet6
    IFL Input Filter Name: L2BSA-FWF-in-10048-ge-1/2/4.3221225472-in
    IFL Output Filter Name: L2BSA-FWF-out-25088-ge-1/2/4.3221225472-out
show subscribers extensive (Subscriber Session Using PCEF Profile)

user@host> show subscribers extensive

Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225517
Interface type: Dynamic
Underlying Interface: ge-1/0/3
Dynamic Profile Name: svlan-dhcp
State: Active
Session ID: 59
PFE Flow ID: 71
Stacked VLAN Id: 0x8100.1
VLAN Id: 0x8100.2
Login Time: 2017-03-28 08:23:08 PDT

Type: DHCP
User Name: pcefuser
IP Address: 192.0.2.26
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225518
Interface type: Dynamic
Underlying Interface: demux0.3221225517
Dynamic Profile Name: dhcp-client-prof
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 60
Session ID: 60
PFE Flow ID: 73
Stacked VLAN Id: 1
VLAN Id: 2
Login Time: 2017-03-28 08:23:08 PDT
Service Sessions: 1
show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail

Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic

**Interface Set:** aci-1003-ge-1/0/0.4001  
**Interface Set Type:** Dynamic  
**Interface Set Session ID:** 13

Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address:
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT

`show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)`

user@host> `show subscribers agent-circuit-identifier aci-ppp-vlan detail`

Type: VLAN  
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13

**Agent Circuit ID:** aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:52
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT

show subscribers id accounting-statistics
user@host> show subscribers id 601 accounting-statistics

Session ID: 601
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

show subscribers interface accounting-statistics
user@host> show subscribers interface pp0.3221226949 accounting-statistics

Session ID: 501
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 502
Accounting Statistics:
Input bytes : 87654
Output bytes : 72108
Input packets: 3322
Output packets: 3322
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 503
Accounting Statistics:
Input bytes : 156528
Output bytes : 123865
Input packets: 7448
Output packets: 7448
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

show subscribers interface extensive
user@host> show subscribers interface demux0.1073741826 extensive

Type: VLAN
User Name: user@test.example.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST
Type: DHCP
User Name: user@test.example.com
IP Address: 192.0.2.0
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2
Service Session ID: 25
Service Session Name: SUB-QOS
State: Active
Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out

show subscribers logical-system terse

user@host>  show subscribers logical-system test1 terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address/VLAN ID</th>
<th>User Name</th>
<th>LS:RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>demux0.1073741825</td>
<td>203.0.113.3</td>
<td>RETAILER1-CLIENT</td>
<td>test1:retailer1</td>
</tr>
<tr>
<td>demux0.1073741826</td>
<td>203.0.113.4</td>
<td>RETAILER2-CLIENT</td>
<td>test1:retailer2</td>
</tr>
</tbody>
</table>

show subscribers physical-interface count

user@host>  show subscribers physical-interface ge-1/0/0 count

Total subscribers: 3998, Active Subscribers: 3998
show subscribers routing-instance inst1 count

user@host> show subscribers routing-instance inst1 count

Total Subscribers: 188, Active Subscribers: 183

show subscribers stacked-vlan-id detail

user@host> show subscribers stacked-vlan-id 101 detail

Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail

Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail

Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
show subscribers user-name detail

user@host> show subscribers user-name larry1 detail

Type: DHCP
User Name: larry1
IP Address: 203.0.113.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c

show subscribers vlan-id

user@host> show subscribers vlan-id 100

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP Address</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/0.1073741824</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-1/2/0.1073741825</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show subscribers vlan-id detail

user@host> show subscribers vlan-id 100 detail

Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
**State:** Active  
**VLAN Id:** 100  
**Login Time:** 2009-03-11 06:48:54 PDT

**Type:** VLAN  
**Interface:** ge-1/2/0.1073741825  
**Interface type:** Dynamic  
**Dynamic Profile Name:** vlan-prof-tpid  
**State:** Active  
**VLAN Id:** 100  
**Login Time:** 2009-03-11 06:48:54 PDT

**show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)**

```
user@host> show subscribers vpi 40 vci 50 extensive
```

**Type:** PPPoE  
**User Name:** testuser  
**IP Address:** 203.0.113.2  
**IP Netmask:** 255.255.0.0  
**Logical System:** default  
**Routing Instance:** default  
**Interface:** pp0.0  
**Interface type:** Static  
**MAC Address:** 00:00:5e:00:53:02  
**State:** Active  
**Radius Accounting ID:** 2  
**Session ID:** 2  
**ATM VPI:** 40  
**ATM VCI:** 50  
**Login Time:** 2012-12-03 07:49:26 PST  
**IP Address Pool:** pool_1  
**IPv6 Framed Interface Id:** 200:65ff:fe23:102

**show subscribers address detail (Enhanced Subscriber Management)**

```
user@host> show subscribers address 203.0.113.111 detail
```

**Type:** DHCP  
**User Name:** simple_filters_service  
**IP Address:** 203.0.113.111  
**IP Netmask:** 255.0.0.0  
**Logical System:** default
Routing Instance: default
Interface: demux0.3221225482
Interface type: Dynamic
Underlying Interface: demux0.3221225472
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:0f
State: Active
Radius Accounting ID: 11
Session ID: 11
PFE Flow ID: 15
Stacked VLAN Id: 210
VLAN Id: 209
Service Sessions: 1
DHCP Options: len 3
35 01 01
show system autorecovery state

Syntax

```
show system autorecovery state
```

Release Information
Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description
Perform checks and show status of all autorecovered items.

Required Privilege Level
view

RELATED DOCUMENTATION
request system autorecovery state | 2519

List of Sample Output
show system autorecovery state on page 2855

Output Fields
Table 110 on page 2854 lists the output fields for the `show system autorecovery state` command. Output fields are listed in the approximate order in which they appear.

Table 110: show system autorecovery state Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>The name of the file on which autorecovery checks are performed.</td>
</tr>
<tr>
<td>Slice</td>
<td>The disk partition on which autorecovery checks are performed.</td>
</tr>
<tr>
<td>Recovery Information</td>
<td>Indicates whether autorecovery information for the file or slice has been saved.</td>
</tr>
<tr>
<td>Integrity Check</td>
<td>Displays the status of the file's integrity check (passed or failed).</td>
</tr>
<tr>
<td>Action / Status</td>
<td>Displays the status of the item, or the action required to be taken for that item.</td>
</tr>
</tbody>
</table>
Sample Output

show system autorecovery state

user@host> show system autorecovery state

<table>
<thead>
<tr>
<th>Configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
</tr>
<tr>
<td>rescue.conf.gz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Licenses:</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
</tr>
<tr>
<td>JUNOS282736.lic</td>
</tr>
<tr>
<td>JUNOS282737.lic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BSD Labels:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slice</td>
</tr>
<tr>
<td>s1</td>
</tr>
<tr>
<td>s2</td>
</tr>
<tr>
<td>s3</td>
</tr>
<tr>
<td>s4</td>
</tr>
</tbody>
</table>
show system download

Syntax

```
show system download <download-id>
```

Release Information
Command introduced in Junos OS Release 11.2 for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

Description
Display a brief summary of all the download instances along with their current state and extent of progress. If a `download-id` is provided, the command displays a detailed report of the particular download instance.

Options
- `download-id`—(Optional) The ID number of the download instance.

Required Privilege Level
view

RELATED DOCUMENTATION

- `request system download start` | 2531

List of Sample Output

- `show system download` on page 2857
- `show system download 1` on page 2857

Output Fields

Table 111 on page 2856 lists the output fields for the `show system download` command. Output fields are listed in the approximate order in which they appear.

**Table 111: show system download Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Displays the download identification number.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the state of a particular download.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Displays the start time of a particular download.</td>
</tr>
</tbody>
</table>
Table 111: show system download Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Progress</strong></td>
<td>Displays the percentage of a download that has been completed.</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Displays the URL from which the file was downloaded.</td>
</tr>
</tbody>
</table>

---

**Sample Output**

**show system download**

user@host> `show system download`

<table>
<thead>
<tr>
<th>Download Status Information:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Status</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>Active</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
</tr>
<tr>
<td>4</td>
<td>Completed</td>
</tr>
</tbody>
</table>

**show system download 1**

user@host> `show system download 1`

<table>
<thead>
<tr>
<th>Download ID</th>
<th>Status</th>
<th>Progress</th>
<th>URL</th>
<th>Local Path</th>
<th>Maximum Rate</th>
<th>Creation Time</th>
<th>Scheduled Time</th>
<th>Start Time</th>
<th>Error Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Active</td>
<td>6%</td>
<td>ftp://ftp-server//tftpboot/1m_file</td>
<td>/var/tmp/1m_file</td>
<td>1k</td>
<td>May 4 06:28:36</td>
<td>May 4 06:28:36</td>
<td>May 4 06:28:37</td>
<td>0</td>
</tr>
</tbody>
</table>
show system license (View)

Syntax

show system license
<installed | keys | status | usage>

Release Information
Command introduced in Junos OS Release 9.5. Logical system status option added in Junos OS Release 11.2.

Description
Display licenses and information about how licenses are used.

Options
none—Display all license information.

installed—(Optional) Display installed licenses only.

keys—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.

status—(Optional) Display license status for a specified logical system or for all logical systems.

usage—(Optional) Display the state of licensed features.

Required Privilege Level
view

RELATED DOCUMENTATION

Adding New Licenses (CLI Procedure)

List of Sample Output
show system license on page 2859
show system license installed on page 2860
show system license keys on page 2860
show system license usage on page 2861
show system license status logical-system all on page 2861

Output Fields
Table 112 on page 2859 lists the output fields for the show system license command. Output fields are listed in the approximate order in which they appear.
Table 112: show system license Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature name</td>
<td>Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.</td>
</tr>
<tr>
<td>Licenses used</td>
<td>Number of licenses used by the device. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.</td>
</tr>
<tr>
<td>Licenses installed</td>
<td>Information about the installed license key:</td>
</tr>
<tr>
<td></td>
<td>• License identifier—Identifier associated with a license key.</td>
</tr>
<tr>
<td></td>
<td>• License version—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.</td>
</tr>
<tr>
<td></td>
<td>• Valid for device—Device that can use a license key.</td>
</tr>
<tr>
<td></td>
<td>• Features—Feature associated with a license.</td>
</tr>
<tr>
<td>Licenses needed</td>
<td>Number of licenses required for features being used but not yet properly licensed.</td>
</tr>
<tr>
<td>Expiry</td>
<td>Time remaining in the grace period before a license is required for a feature being used.</td>
</tr>
<tr>
<td>Logical system</td>
<td>Displays whether a license is enabled for a logical system.</td>
</tr>
<tr>
<td>license status</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show system license

user@host> show system license

License usage:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses used</th>
<th>Licenses installed</th>
<th>Licenses needed</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>av_key_kaspersky_engine</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2012-03-30 01:00:00 IST</td>
</tr>
<tr>
<td>wf_key_surfcontrol_cpa</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2012-03-30 01:00:00 IST</td>
</tr>
<tr>
<td>dynamic-vpn</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>ax411-wlan-ap</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
</tbody>
</table>
Licenses installed:
  License identifier: JUNOS301998
  License version: 2
  Valid for device: AG4909AA0080
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

License identifier: JUNOS302000
License version: 2
Valid for device: AG4909AA0080
Features:
  wf_key_surfcontrol_cpa - Web Filtering
    date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

show system license installed

user@host> show system license installed

License identifier: JUNOS301998
License version: 2
Valid for device: AG4909AA0080
Features:
  av_key_kaspersky_engine - Kaspersky AV
    date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

License identifier: JUNOS302000
License version: 2
Valid for device: AG4909AA0080
Features:
  wf_key_surfcontrol_cpa - Web Filtering
    date-based, 2011-03-30 01:00:00 IST - 2012-03-30 01:00:00 IST

show system license keys

user@host> show system license keys

XXXXXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
  xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
**show system license usage**

```
user@host> show system license usage
```

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses used</th>
<th>Licenses installed</th>
<th>Licenses needed</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>av_key_kaspersky_engine</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2012-03-30</td>
</tr>
<tr>
<td>wf_key_surfcontrol_cpa</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2012-03-30</td>
</tr>
<tr>
<td>dynamic-vpn</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>ax411-wlan-ap</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
</tbody>
</table>

**show system license status logical-system all**

```
user@host> show system license status logical-system all
```

**Logical system license status:**

<table>
<thead>
<tr>
<th>logical system name</th>
<th>license status</th>
</tr>
</thead>
<tbody>
<tr>
<td>root-logical-system</td>
<td>enabled</td>
</tr>
<tr>
<td>LSYS0</td>
<td>enabled</td>
</tr>
<tr>
<td>LSYS1</td>
<td>enabled</td>
</tr>
<tr>
<td>LSYS2</td>
<td>enabled</td>
</tr>
</tbody>
</table>
show system login lockout

Syntax

show system login lockout

Release Information
Command introduced in Junos OS Release 11.2.

Description
Display the usernames locked after unsuccessful login attempts.

Required Privilege Level
view and system

RELATED DOCUMENTATION

<table>
<thead>
<tr>
<th>lockout-period</th>
<th>1920</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear system login lockout</td>
<td>2489</td>
</tr>
</tbody>
</table>

List of Sample Output
show system login lockout on page 2863

Output Fields
Table 113 on page 2862 lists the output fields for the show system login lockout command. Output fields are listed in the approximate order in which they appear.

Table 113: show system login lockout

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Username</td>
<td>All levels</td>
</tr>
<tr>
<td>Lockout start</td>
<td>Date and time the username was locked</td>
<td>All levels</td>
</tr>
<tr>
<td>Lockout end</td>
<td>Date and time the username was unlocked</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Sample Output

```console
show system login lockout

user@host> show system login lockout

<table>
<thead>
<tr>
<th>User</th>
<th>Lockout start</th>
<th>Lockout end</th>
</tr>
</thead>
</table>
```
**show system services dhcp binding**

**Syntax**

```
show system services dhcp binding
<detail>
<address>
```

**Release Information**

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

**Description**

(EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.

**Options**

- `none`—Display brief information about all active client bindings.
- `detail`—(Optional) Display detailed information about all active client bindings.
- `address`—(Optional) Display detailed client binding information for the specified IP address only.

**Required Privilege Level**

view and system

**RELATED DOCUMENTATION**

| clear system services dhcp binding | 2490 |

**List of Sample Output**

| show system services dhcp binding on page 2865 |
| show system services dhcp binding address on page 2866 |
| show system services dhcp binding address detail on page 2866 |

**Output Fields**

Table 114 on page 2865 describes the output fields for the `show system services dhcp binding` command. Output fields are listed in the approximate order in which they appear.
Table 114: show system services dhcp binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated address</td>
<td>List of IP addresses the DHCP server has assigned to clients.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>Corresponding media access control (MAC) hardware address of the client.</td>
<td>All levels</td>
</tr>
<tr>
<td>Client identifier</td>
<td><em>(address option only)</em> Client’s unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings.</td>
<td>All levels</td>
</tr>
<tr>
<td>Binding Type</td>
<td>Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.</td>
<td>All levels</td>
</tr>
<tr>
<td>Lease Expires at</td>
<td>Time the lease expires or <em>never</em> for leases that do not expire.</td>
<td>All levels</td>
</tr>
<tr>
<td>Lease Obtained at</td>
<td><em>(address option only)</em> Time the client obtained the lease from the DHCP server.</td>
<td>detail</td>
</tr>
<tr>
<td>State</td>
<td>Status of the binding. Bindings can be active or expired.</td>
<td>detail</td>
</tr>
<tr>
<td>Pool</td>
<td>Address pool that contains the IP address assigned to the client.</td>
<td>detail</td>
</tr>
<tr>
<td>Request received on</td>
<td>Interface on which the DHCP message exchange occurs. The IP address pool is configured based on the interface's IP address. If a relay agent is used, its IP address is also displayed.</td>
<td>detail</td>
</tr>
<tr>
<td>DHCP options</td>
<td>User-defined options created for the DHCP server. If no options have been defined, this field is blank.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

```
show system services dhcp binding
user@host> show system services dhcp binding

Allocated address   MAC address        Binding Type   Lease expires at
192.168.1.2          00:a0:12:00:12:ab  static         never
192.168.1.3          00:a0:12:00:13:02  dynamic        2004-05-03 13:01:42 PDT
```
show system services dhcp binding address

user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00
3a 31 33 3a 30 32:13:02

Lease information:
    Binding Type dynamic
    Obtained at 2004-05-02 13:01:42 PDT
    Expires at 2004-05-03 13:01:42 PDT

show system services dhcp binding address detail

user@host> show system services dhcp binding 192.168.1.3 detail

DHCP binding information:
Allocated address 192.168.1.3
Mac address 00:a0:12:00:12:ab
Pool 192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254

Lease information:
    Type DHCP
    Obtained at 2004-05-02 13:01:42 PDT
    Expires at 2004-05-03 13:01:42 PDT
    State active

DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
    Name: domain-name, Value: mydomain.tld
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 3.3.3.33
**show system services dhcp client**

**Syntax**

```
show system services dhcp client
  < interface-name >
  <statistics>
```

**Release Information**

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display information about DHCP clients.

**Options**

- none—Display DHCP information for all interfaces.
- *interface-name*—(Optional) Display DHCP information for the specified interface.

**Required Privilege Level**

view and system

**RELATED DOCUMENTATION**

- *dhcp (Interfaces)*
- request system services dhcp | 2549

**List of Sample Output**

- *show system services dhcp client on page 2869*
- *show system services dhcp client ge-0/0/34.0 on page 2870*
- *show system services dhcp client statistics on page 2870*

**Output Fields**

*Table 115 on page 2868* lists the output fields for the *show system services dhcp client* command. Output fields are listed in the approximate order in which they appear.
Table 115: show system services dhcp client Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface Name</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>Client Status</td>
<td>State of the client binding.</td>
</tr>
<tr>
<td>Vendor Identifier</td>
<td>Vendor ID.</td>
</tr>
<tr>
<td>Server Address</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>Address obtained</td>
<td>IP address obtained from the DHCP server.</td>
</tr>
<tr>
<td>Lease Obtained at</td>
<td>Date and time the lease was obtained.</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>(EX Series switches only) Time the current lease expires in (seconds).</td>
</tr>
<tr>
<td>Lease Expires at</td>
<td>Date and time the lease expires.</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>• Name: server-identifier, Value: IP address of the name server.</td>
</tr>
<tr>
<td></td>
<td>• Name: device, Value: IP address of the name device.</td>
</tr>
<tr>
<td></td>
<td>• Name: domain-name, Value: Name of the domain.</td>
</tr>
<tr>
<td>Packets dropped</td>
<td>Total packets dropped.</td>
</tr>
<tr>
<td>Messages received</td>
<td>Number of the following DHCP messages received:</td>
</tr>
<tr>
<td></td>
<td>• DHCPOFFER—First packet received on a logical interface when DHCP is enabled.</td>
</tr>
<tr>
<td></td>
<td>• DHCPACK—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stops the earlier timer added for DHCPACK.</td>
</tr>
<tr>
<td></td>
<td>• DHCPNAK—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.</td>
</tr>
</tbody>
</table>
Table 115: show system services dhcp client Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages sent</td>
<td>Number of the following DHCP messages sent:</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPDECLINE</strong>—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPDISCOVER</strong>—Packet sent on the interface for which the DHCP client is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPREQUEST</strong>—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPINFORM</strong>—Packet sent to the DHCP server for local configuration parameters.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPRELEASE</strong>—Packet sent to the DHCP server to relinquish network address and cancel remaining lease.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPRENEW</strong>—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPOFFER message, which will be unicast directly to the server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPREBIND</strong>—Packet sent to any server to renew the address. The next message to be sent will be a DHCPOFFER message, which will be broadcast.</td>
</tr>
</tbody>
</table>

Sample Output

```
show system services dhcp client

user@host> show system services dhcp client

Logical Interface name         ge-0/0/34.0
Hardware address        00:1f:12:38:5f:e5
Client status           bound
Address obtained        10.0.0.2
Update server           disabled
Lease obtained at       2013-12-23 08:11:40 UTC
Lease expires in        93
Lease expires at        2013-12-23 08:13:20 UTC

DHCP options:
  Name: server-identifier, Value: 10.0.0.1
  Code: 1, Type: ip-address, Value: 255.255.255.0
```
### Sample Output

**show system services dhcp client ge-0/0/34.0**

```
user@host> show system services dhcp client ge-0/0/34.0
```

<table>
<thead>
<tr>
<th>Logical Interface name</th>
<th>ge-0/0/34.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware address</td>
<td>00:1f:12:38:5f:e5</td>
</tr>
<tr>
<td>Client status</td>
<td>bound</td>
</tr>
<tr>
<td>Address obtained</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>Update server</td>
<td>disabled</td>
</tr>
<tr>
<td>Lease obtained at</td>
<td>2013-12-23 08:11:40 UTC</td>
</tr>
<tr>
<td>Lease expires in</td>
<td>87</td>
</tr>
<tr>
<td>Lease expires at</td>
<td>2013-12-23 08:13:20 UTC</td>
</tr>
</tbody>
</table>

DHCP options:
- Name: server-identifier, Value: 10.0.0.1
- Code: 1, Type: ip-address, Value: 255.255.255.0

### Sample Output

**show system services dhcp client statistics**

```
user@host> show system services dhcp client statistics
```

<table>
<thead>
<tr>
<th>Packets dropped:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages received:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPOFFER</td>
</tr>
<tr>
<td>DHCPACK</td>
</tr>
<tr>
<td>DHCPNAK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Messages sent:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDECLINE</td>
</tr>
<tr>
<td>DHCPDISCOVER</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
</tr>
<tr>
<td>DHCPINFORM</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
</tr>
<tr>
<td>DHCPRENEW</td>
</tr>
<tr>
<td>DHCPREBIND</td>
</tr>
</tbody>
</table>
show system services dhcp conflict

Syntax

```
show system services dhcp conflict
```

Release Information

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

Description

(J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool.

Options

This command has no options.

Required Privilege Level

view and system

RELATED DOCUMENTATION

| clear system services dhcp conflict | 2491 |

List of Sample Output

show system services dhcp conflict on page 2872

Output Fields

Table 116 on page 2871 describes the output fields for the `show system services dhcp conflict` command. Output fields are listed in the approximate order in which they appear.

Table 116: show system services dhcp conflict Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection time</td>
<td>Date and time the client detected the conflict.</td>
</tr>
<tr>
<td>Detection method</td>
<td>How the conflict was detected.</td>
</tr>
</tbody>
</table>
Table 116: show system services dhcp conflict Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a clear system services dhcp conflict command to manually clear the list.</td>
</tr>
</tbody>
</table>

Sample Output

code

```
show system services dhcp conflict

user@host> show system services dhcp conflict

<table>
<thead>
<tr>
<th>Detection time</th>
<th>Detection method</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-08-03 19:04:00 PDT</td>
<td>ARP</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>2004-08-04 04:23:12 PDT</td>
<td>Ping</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>2004-08-05 21:06:44 PDT</td>
<td>Client</td>
<td>10.0.0.3</td>
</tr>
</tbody>
</table>
```
show system services dhcp global

Syntax

```
show system services dhcp global
```

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

Description
(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients.

Options
This command has no options.

Required Privilege Level
view and system

List of Sample Output
show system services dhcp global on page 2874

Output Fields
Table 117 on page 2873 describes the output fields for the show system services dhcp global command. Output fields are listed in the approximate order in which they appear.

Table 117: show system services dhcp global Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTP lease length</td>
<td>Length of lease time assigned to BOOTP clients.</td>
</tr>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
</tr>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client retains an IP address lease on the server.</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
</tr>
</tbody>
</table>
Table 117: show system services dhcp global Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP options</strong></td>
<td>User-defined options created for the DHCP server. If no options have been defined, this field is blank.</td>
</tr>
</tbody>
</table>

Sample Output

show system services dhcp global

user@host> show system services dhcp global

Global settings:
  BOOTP lease length infinite

DHCP lease times:
  Default lease time 1 hour
  Minimum lease time 2 hours
  Maximum lease time infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.33
show system services dhcp pool

Syntax

```
show system services dhcp pool
  <detail>
  <subnet-address>
```

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

Description
(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools.

Options

- **none**—Display brief information about all IP address pools.
- **detail**—(Optional) Display detailed information.
- **subnet-address**—(Optional) Display information for the specified subnet address.

Required Privilege Level

view and system

List of Sample Output

- show system services dhcp pool on page 2876
- show system services dhcp pool subnet-address on page 2877
- show system services dhcp pool subnet-address detail on page 2877

Output Fields

Table 118 on page 2875 describes the output fields for the show system services dhcp pool command. Output fields are listed in the approximate order in which they appear.

Table 118: show system services dhcp pool Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool name</td>
<td>Subnet on which the IP address pool is defined.</td>
<td>None specified</td>
</tr>
<tr>
<td>Low address</td>
<td>Lowest address in the IP address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>High address</td>
<td>Highest address in the IP address pool.</td>
<td>None specified</td>
</tr>
</tbody>
</table>
Table 118: show system services dhcp pool Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluded addresses</td>
<td>Addresses excluded from the address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>Subnet</td>
<td><em>(subnet-address</em> option only) Subnet to which the specified address pool belongs.</td>
<td>None specified</td>
</tr>
<tr>
<td>Address range</td>
<td><em>(subnet-address</em> option only) Range of IP addresses in the address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>Addresses assigned</td>
<td>Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool.</td>
<td>detail</td>
</tr>
<tr>
<td>Active</td>
<td>Number of assigned IP addresses in the pool that are active.</td>
<td>detail</td>
</tr>
<tr>
<td>Excluded</td>
<td>Number of assigned IP addresses in the pool that are excluded.</td>
<td>detail</td>
</tr>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
<td>detail</td>
</tr>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client can retain an IP address lease on the server.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
<td>detail</td>
</tr>
<tr>
<td>DHCP options</td>
<td>User-defined options created for the DHCP server. If no options have been defined, this field is blank.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show system services dhcp pool

user@host> show system services dhcp pool

<table>
<thead>
<tr>
<th>Pool name</th>
<th>Low address</th>
<th>High address</th>
<th>Excluded addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.0/24</td>
<td>192.0.2.2</td>
<td>192.0.2.254</td>
<td>192.0.2.1</td>
</tr>
</tbody>
</table>
show system services dhcp pool subnet-address

user@host> show system services dhcp pool 192.0.2.0/24

Pool information:
- Subnet: 192.0.2.0/24
- Address range: 192.0.2.2 - 192.0.2.254
- Addresses assigned: 2/253

show system services dhcp pool subnet-address detail

user@host> show system services dhcp pool 192.0.2.0/24 detail

Pool information:
- Subnet: 192.0.2.0/24
- Address range: 192.0.2.2 - 192.0.2.254
- Addresses assigned: 2/253
  - Active: 1, Excluded: 1

DHCP lease times:
- Default lease time: 1 hour
- Minimum lease time: 2 hours
- Maximum lease time: infinite

DHCP options:
- Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
- Name: domain-name, Value: mydomain.tld
- Name: router, Value: { 192.0.2.1 }
- Name: server-identifier, Value: 192.0.2.1
- Code: 19, Type: flag, Value: off
- Code: 40, Type: string, Value: domain.tld
- Code: 32, Type: ip-address, Value: 192.0.2.1
show system services dhcp relay-statistics

Syntax

```
show system services dhcp relay-statistics
```

Release Information
Command introduced in Junos OS Release 8.5.

Description
Display information about the DHCP relay.

Required Privilege Level
view and system

RELATED DOCUMENTATION

| dhcp |

List of Sample Output

```
show system services dhcp relay-statistics on page 2879
```

Output Fields

Table 119 on page 2878 lists the output fields for the `show system services dhcp relay-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 119: show system services dhcp relay-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received packets</td>
<td>Total DHCP packets received.</td>
</tr>
<tr>
<td>Forwarded packets</td>
<td>Total DHCP packet forwarded.</td>
</tr>
</tbody>
</table>
### Table 119: show system services dhcp relay-statistics Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dropped packets</strong></td>
<td>Total DHCP packets dropped for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to a missing interface in the relay database</strong>—Number of packets discarded</td>
</tr>
<tr>
<td></td>
<td>because they did not belong to a configured interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to a missing matching routing instance</strong>—Number of packets discarded</td>
</tr>
<tr>
<td></td>
<td>because they did not belong to a configured routing instance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to an error during packet read</strong>—Number of packets discarded because of</td>
</tr>
<tr>
<td></td>
<td>a system read error.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to an error during packet send</strong>—Number of packets that the DHCP relay</td>
</tr>
<tr>
<td></td>
<td>application could not send.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to an invalid server address</strong>—Number of packets discarded because an</td>
</tr>
<tr>
<td></td>
<td>invalid server address was specified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to a missing valid local address</strong>—Number of packets discarded because</td>
</tr>
<tr>
<td></td>
<td>there was no valid local address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Due to a missing route to the server or client</strong>—Number of packets discarded</td>
</tr>
<tr>
<td></td>
<td>because there were no addresses available for assignment.</td>
</tr>
</tbody>
</table>

---

### Sample Output

**show system services dhcp relay-statistics**

```
user@host> show system services dhcp relay-statistics

Received packets: 4
Forwarded packets: 4
Dropped packets: 4
  Due to missing interface in relay database: 4
  Due to missing matching routing instance: 0
  Due to an error during packet read: 0
  Due to an error during packet send: 0
  Due to invalid server address: 0
  Due to missing valid local address: 0
  Due to missing route to server/client: 0
```
show system services dhcp statistics

Syntax

show system services dhcp statistics

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

Description
(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics.

Options
This command has no options.

Required Privilege Level
view and system

RELATED DOCUMENTATION

| clear system services dhcp statistics | 2492 |

List of Sample Output
show system services dhcp statistics on page 2881

Output Fields
Table 120 on page 2880 describes the output fields for the show system services dhcp statistics command. Output fields are listed in the approximate order in which they appear.

Table 120: show system services dhcp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
</tr>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client can retain an IP address lease on the server.</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
</tr>
</tbody>
</table>
Table 120: show system services dhcp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets dropped</strong></td>
<td>Total number of packets dropped and number of packets dropped because of:</td>
</tr>
<tr>
<td></td>
<td>• Invalid hardware address</td>
</tr>
<tr>
<td></td>
<td>• Invalid opcode</td>
</tr>
<tr>
<td></td>
<td>• Invalid server address</td>
</tr>
<tr>
<td></td>
<td>• No available address</td>
</tr>
<tr>
<td></td>
<td>• No interface match</td>
</tr>
<tr>
<td></td>
<td>• No routing instance match</td>
</tr>
<tr>
<td></td>
<td>• No valid local addresses</td>
</tr>
<tr>
<td></td>
<td>• Packet too short</td>
</tr>
<tr>
<td></td>
<td>• Read error</td>
</tr>
<tr>
<td></td>
<td>• Send error</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of the following message types sent from DHCP clients and received by the DHCP server:</td>
</tr>
<tr>
<td></td>
<td>• BOOTREQUEST</td>
</tr>
<tr>
<td></td>
<td>• DHCPDECLINE</td>
</tr>
<tr>
<td></td>
<td>• DHCPDISCOVER</td>
</tr>
<tr>
<td></td>
<td>• DHCPINFORM</td>
</tr>
<tr>
<td></td>
<td>• DHCPRELEASE</td>
</tr>
<tr>
<td></td>
<td>• DHCPREQUEST</td>
</tr>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of the following message types sent from the DHCP server to DHCP clients:</td>
</tr>
<tr>
<td></td>
<td>• BOOTREPLY</td>
</tr>
<tr>
<td></td>
<td>• DHCPACK</td>
</tr>
<tr>
<td></td>
<td>• DHCPOFFER</td>
</tr>
<tr>
<td></td>
<td>• DHCPNAK</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show system services dhcp statistics
user@host> show system services dhcp statistics
```
DHCP lease times:
- Default lease time: 1 hour
- Minimum lease time: 2 hours
- Maximum lease time: infinite

Packets dropped:
- Total: 0
- Bad hardware address: 0
- Bad opcode: 0
- Invalid server address: 0
- No available addresses: 0
- No interface match: 0
- No routing instance match: 0
- No valid local address: 0
- Packet too short: 0
- Read error: 0
- Send error: 0

Messages received:
- BOOTREQUEST: 0
- DHCPDECLINE: 0
- DHCPDISCOVER: 0
- DHCPINFORM: 0
- DHCPRELEASE: 0
- DHCPREQUEST: 0

Messages sent:
- BOOTREPLY: 0
- DHCPACK: 0
- DHCPOFFER: 0
- DHCPNAK: 0
**show system services service-deployment**

**Syntax**

```
show system services service-deployment
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display information about a Session and Resource Control (SRC) client.

**Options**

This command has no options.

**Required Privilege Level**

system
view

**List of Sample Output**

*show system services service-deployment on page 2884*

**Output Fields**

*Table 121 on page 2883 lists the output fields for the show system services service-deployment command. Output fields are listed in the approximate order in which they appear.*

**Table 121: show system services service-deployment Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDT Keepalive settings</td>
<td>Configured PDT keepalive interval, in seconds.</td>
</tr>
<tr>
<td>Keepalives sent</td>
<td>Number of keepalives sent.</td>
</tr>
<tr>
<td>Notifications sent</td>
<td>Number of notifications sent.</td>
</tr>
<tr>
<td>Last update from peer</td>
<td>Time at which the last update from a peer was received.</td>
</tr>
</tbody>
</table>
Sample Output

```
show system services service-deployment

user@host> show system services service-deployment

Connected to 192.0.2.0 port 10288 since 2004-05-03 11:04:34 PDT Keepalive settings:
Interval 15 seconds Keepalives sent: 750 Notifications sent: 0 Last update from peer: 00:00:06 ago
```
show system snapshot media

Syntax

```
show system snapshot < media (compact-flash | external | harddisk | internal | usb) >
```

Release Information
Command introduced in Junos OS Release 10.2.

Description
Display information about the partitioning scheme present on the media. Information for only one root is displayed for single-root partitioning, whereas information for both roots is displayed for dual-root partitioning.

Options
- compact-flash— Show snapshot information from the CompactFlash card. (Supported on SRX5400, SRX5600, SRX5800)
- external— Show snapshot information from the external CompactFlash card. (Not supported on SRX5000 Series devices)
- hard-disk— Show snapshot information from the Hard Disk. (Supported on SRX5400, SRX5600, SRX5800)
- internal— Show snapshot information from internal media. (Not supported on SRX5000 Series devices)
- usb— Show snapshot information from device connected to USB port.

Required Privilege Level
View

RELATED DOCUMENTATION

Creating a Snapshot and Using It to Boot an SRX Series device

List of Sample Output
show system snapshot media compact-flash on page 2886
show system snapshot media external on page 2886
show system snapshot media internal on page 2886
show system snapshot media usb on page 2887
show system snapshot media hard-disk on page 2887

Output Fields
Table 122 on page 2886 lists the output fields for the `show system snapshot media` command. Output fields are listed in the approximate order in which they appear.

**Table 122: show system snapshot media Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation date</td>
<td>Date and time of the last snapshot.</td>
</tr>
<tr>
<td>JUNOS version on snapshot</td>
<td>Junos OS release number of individual software packages.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show system snapshot media compact-flash
show system snapshot media compact-flash
Information for snapshot on compact-flash (ad0s1)
Creation date: Aug 21 11:58:14 2017
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic

show system snapshot media external
show system snapshot media external
Information for snapshot on external (/dev/da1s2a) (primary)
Creation date: Apr 9 09:41:16 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic
Information for snapshot on external (/dev/da1s1a) (backup)
Creation date: Apr 9 09:41:16 2018
JUNOS version on snapshot:
  junos  : 12.3X48-D40.5-domestic

show system snapshot media internal
show system snapshot media internal
Information for snapshot on internal (/dev/da0s1a) (primary)
Creation date: Jan 15 10:43:26 2010
JUNOS version on snapshot:
```
show system snapshot media usb

show system snapshot media usb

Information for snapshot on usb (da0s1)
Creation date: Apr 9 08:44:46 2018
JUNOS version on snapshot:
  junos : 12.3X48-D40.5-domestic

show system snapshot media hard-disk

show system snapshot media hard-disk

Information for snapshot on hard-disk (ad2s1)
Creation date: Apr 9 16:40:18 2018
JUNOS version on snapshot:
  junos : 12.3X48-D40.5-domestic
show system storage partitions

List of Syntax
Syntax (EX Series) on page 2888
Syntax (SRX Series) on page 2888

Syntax (EX Series)

show system storage partitions
<all-members>
<local>
<member member-id>

Syntax (SRX Series)

show system storage partitions

Release Information
Command introduced in Junos OS Release 10.2 for SRX300, SRX320, SRX340, SRX345, and SRX550HM devices.
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description
Display information about the disk partitioning scheme.

Options
none—Display partition information.

all-members—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.

local—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.

member member-id—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.

Required Privilege Level
view

RELATED DOCUMENTATION
Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch

Example: Installing Junos OS on SRX Series Devices Using the Partition Option

[EX] Switch boots from backup root partition after file system corruption occurred on the primary root partition

List of Sample Output

- show system storage partitions (EX Series) on page 2889
- show system storage partitions (SRX Series, Dual Root Partitioning) on page 2890
- show system storage partitions (SRX Series, Single Root Partitioning) on page 2890
- show system storage partitions (SRX Series, USB) on page 2891

Output Fields

Table 123 on page 2889 describes the output fields for the `show system storage partitions` command. Output fields are listed in the approximate order in which they appear.

Table 123: show system storage partitions Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Media</td>
<td>Media (internal or external) from which the switch was booted.</td>
</tr>
<tr>
<td>Active Partition</td>
<td>Name of the active root partition.</td>
</tr>
<tr>
<td>Backup Partition</td>
<td>Name of the backup (alternate) root partition.</td>
</tr>
<tr>
<td>Currently booted from</td>
<td>Partition from which the switch was last booted.</td>
</tr>
<tr>
<td>Partitions information</td>
<td>Information about partitions on the boot media:</td>
</tr>
<tr>
<td></td>
<td>• Partition—Partition identifier.</td>
</tr>
<tr>
<td></td>
<td>• Size—Size of partition.</td>
</tr>
<tr>
<td></td>
<td>• Mountpoint—Directory on which the partition is mounted.</td>
</tr>
</tbody>
</table>

Sample Output

- show system storage partitions (EX Series)

  `user@switch> show system storage partitions`

  ```
  fpc0:
  ```
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>184M</td>
<td>/</td>
</tr>
<tr>
<td>s2a</td>
<td>184M</td>
<td>altroot</td>
</tr>
<tr>
<td>s3d</td>
<td>369M</td>
<td>/var/tmp</td>
</tr>
<tr>
<td>s3e</td>
<td>123M</td>
<td>/var</td>
</tr>
<tr>
<td>s4d</td>
<td>62M</td>
<td>/config</td>
</tr>
<tr>
<td>s4e</td>
<td></td>
<td>unused (backup config)</td>
</tr>
</tbody>
</table>

show system storage partitions (SRX Series, Dual Root Partitioning)

show system storage partitions

Boot Media: internal (da0)
Active Partition: da0s2a
Backup Partition: da0s1a
Currently booted from: active (da0s2a)

Partitions Information:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>293M</td>
<td>altroot</td>
</tr>
<tr>
<td>s2a</td>
<td>293M</td>
<td>/</td>
</tr>
<tr>
<td>s3e</td>
<td>24M</td>
<td>/config</td>
</tr>
<tr>
<td>s3f</td>
<td>342M</td>
<td>/var</td>
</tr>
<tr>
<td>s4a</td>
<td>30M</td>
<td>recovery</td>
</tr>
</tbody>
</table>

show system storage partitions (SRX Series, Single Root Partitioning)

show system storage partitions

Boot Media: internal (da0)
Partitions Information:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>898M</td>
<td>/</td>
</tr>
<tr>
<td>s1e</td>
<td>24M</td>
<td>/config</td>
</tr>
<tr>
<td>s1f</td>
<td>61M</td>
<td>/var</td>
</tr>
</tbody>
</table>
show system storage partitions (SRX Series, USB)

show system storage partitions

Boot Media: usb (da1)
Active Partition: da1s1a
Backup Partition: da1s2a
Currently booted from: active (da1s1a)

Partitions Information:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>293M</td>
<td>/</td>
</tr>
<tr>
<td>s2a</td>
<td>293M</td>
<td>altroot</td>
</tr>
<tr>
<td>s3e</td>
<td>24M</td>
<td>/config</td>
</tr>
<tr>
<td>s3f</td>
<td>342M</td>
<td>/var</td>
</tr>
<tr>
<td>s4a</td>
<td>30M</td>
<td>recovery</td>
</tr>
</tbody>
</table>
show system users

List of Syntax
Syntax on page 2892
Syntax (TX Matrix Router) on page 2892
Syntax (TX Matrix Plus Router) on page 2892
Syntax (MX Series Router) on page 2892

Syntax

```
show system users
<nor-resolve>
```

Syntax (TX Matrix Router)

```
show system users
<all-chassis | all-lcc | lcc number | scc>
<nor-resolve>
```

Syntax (TX Matrix Plus Router)

```
show system users
<detail>
<all-chassis | all-lcc | lcc number | sfc number>
<nor-resolve>
```

Syntax (MX Series Router)

```
show system users
<all-members>
<local>
<member member-id>
<nor-resolve>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in JUNOS OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

List information about the users who are currently logged in to the router or switch.
The show system users command lists the information about administrative users that are logged in to a router or switch using the CLI, J-Web, or an SSH client. The output does not list information about web users or automated users that are logged in from a remote client application using Junos XML APIs, such as NETCONF.

Options

- **none**—List information about the users who are currently logged in to the router or switch.

- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show users currently logged in to all the routers in the chassis.

- **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to all connected T1600 or T4000 LCCs.

- **all-members**—(MX Series routers only) (Optional) Display users currently logged in to all members of the Virtual Chassis configuration.

- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to a specific router that is connected to the TX Matrix Plus router.

  Replace number with the following values depending on the LCC configuration:

  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

- **local**—(MX Series routers only) (Optional) Display users currently logged in to the local Virtual Chassis member.

- **member member-id**—(MX Series routers only) (Optional) Display users currently logged in to the specified member of the Virtual Chassis configuration. Replace **member-id** with a value of 0 or 1.

- **no-resolve**—(Optional) Do not attempt to resolve IP addresses to hostnames.

- **scc**—(TX Matrix routers only) (Optional) Show users currently logged in to the TX Matrix router (or switch-card chassis).
**sfc number**—(TX Matrix Plus routersonly) (Optional) Show users currently logged in to the TX Matrix Plus router. Replace **number** with 0.

**Additional Information**
By default, when you issue the **show system users** command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

**Required Privilege Level**
view

**RELATED DOCUMENTATION**

*Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**
show system users on page 2895
show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router) on page 2895
show system users (TX Matrix Plus Router) on page 2895
show system users (QFX Series) on page 2897
show system users no-resolve (QFX Series) on page 2897

**Output Fields**
Table 124 on page 2894 describes the output fields for the **show system users** command. Output fields are listed in the approximate order in which they appear.

**Table 124: show system users Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>time and up</strong></td>
<td>Current time, in the local time zone, and how long the router or switch has been operational.</td>
</tr>
<tr>
<td><strong>users</strong></td>
<td>Number of users logged in to the router or switch.</td>
</tr>
<tr>
<td><strong>load averages</strong></td>
<td>Load averages for the last 1 minute, 5 minutes, and 15 minutes.</td>
</tr>
<tr>
<td><strong>USER</strong></td>
<td>Username.</td>
</tr>
<tr>
<td><strong>TTY</strong></td>
<td>Terminal through which the user is logged in.</td>
</tr>
<tr>
<td><strong>FROM</strong></td>
<td>System from which the user has logged in. A hyphen indicates that the user is logged in through the console.</td>
</tr>
</tbody>
</table>
Table 124: show system users Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGIN@</td>
<td>Time when the user logged in.</td>
</tr>
<tr>
<td>IDLE</td>
<td>How long the user has been idle.</td>
</tr>
<tr>
<td>WHAT</td>
<td>Processes that the user is running.</td>
</tr>
</tbody>
</table>

Sample Output

show system users

user@host> show system users

7:30PM  up 4 days,  2:26,  2 users, load averages: 0.07, 0.02, 0.01
USER     TTY FROM              LOGIN@  IDLE WHAT
root     d0  -                Fri05PM 4days -csh (csh)
blue     p0  level5.company.net 7:30PM     - cli

show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router)

user@host> show system users lcc 2 no-resolve

lcc2-re0:
------------------------------------------------------------------------
10:34AM PDT up 1 day,  7:11,  5 users, load averages: 0.03, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
root     d0       -                                3:21AM   7:12 /bin/csh
user1    p0       scc-re0                          10:15AM     - telnet hostA
user1    p1       scc-re0                          10:16AM     - telnet hostA
user1    p2       scc-re0                          10:19AM     - telnet hostA
user1    p3       scc-re0                          10:24AM     - telnet hostA

show system users (TX Matrix Plus Router)

user@host> show system users
sfc0-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>user2</td>
<td>p0</td>
<td>10.209.208.123</td>
<td>1:18AM</td>
<td>21</td>
<td>cli</td>
</tr>
<tr>
<td>user2</td>
<td>p1</td>
<td>192.0.2.207</td>
<td>1:37AM</td>
<td>2</td>
<td>cli</td>
</tr>
<tr>
<td>user2</td>
<td>p2</td>
<td>192.0.2.19</td>
<td>1:40AM</td>
<td></td>
<td>cli</td>
</tr>
</tbody>
</table>

lcc0-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc1-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc2-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc3-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

user3@aj> show system users

sfc0-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>p0</td>
<td>device1.example.com</td>
<td>1:18AM</td>
<td>22</td>
<td>cli</td>
</tr>
<tr>
<td>user</td>
<td>p1</td>
<td>device2.example.com</td>
<td>1:37AM</td>
<td></td>
<td>cli</td>
</tr>
<tr>
<td>user</td>
<td>p2</td>
<td>device3.example.com</td>
<td>1:40AM</td>
<td></td>
<td>cli</td>
</tr>
<tr>
<td>user</td>
<td>p3</td>
<td>device4.example.com</td>
<td>1:42AM</td>
<td></td>
<td>-csh (csh)</td>
</tr>
</tbody>
</table>

lcc0-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc1-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc2-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>

lcc3-re0:

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
</table>
show system users (QFX Series)

user@switch>  show system users

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>p0</td>
<td>192.0.2.117</td>
<td>2:54AM</td>
<td>39</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>user2</td>
<td>p1</td>
<td>192.0.2.116</td>
<td>3:01AM</td>
<td>-</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>user3</td>
<td>p2</td>
<td>192.0.2.97</td>
<td>3:08AM</td>
<td>11</td>
<td>-cli (cli)</td>
</tr>
</tbody>
</table>

show system users no-resolve (QFX Series)

user@switch>  show system users no-resolve

<table>
<thead>
<tr>
<th>USER</th>
<th>TTY</th>
<th>FROM</th>
<th>LOGIN@</th>
<th>IDLE</th>
<th>WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>p0</td>
<td>192.0.2.117</td>
<td>2:54AM</td>
<td>39</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>user2</td>
<td>p1</td>
<td>192.0.2.116</td>
<td>3:01AM</td>
<td>-</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>user3</td>
<td>p2</td>
<td>192.0.2.97</td>
<td>3:08AM</td>
<td>11</td>
<td>-cli (cli)</td>
</tr>
</tbody>
</table>
ssh

List of Syntax
Syntax on page 2898
Syntax (EX Series Switch and the QFX Series) on page 2898

Syntax

ssh host
  <bypass-routing>
  <inet | inet6>
  <interface interface-name>
  <logical-system logical-system-name>
  <tenant tenant-name>
  <routing-instance routing-instance-name>
  <source address>
  <v2>
  <port port-number>

Syntax (EX Series Switch and the QFX Series)

ssh host
  <bypass-routing>
  <inet | inet6>
  <interface interface-name>
  <routing-instance routing-instance-name>
  <source address>
  <v2>
  <port port-number>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.
The command tenant option is introduced in Junos OS Release 19.2R1 for SRX Series.

Description
Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the ssh command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:
ssh address 'cli-command1 ; cli-command2 ' 

Options
host—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface interface-name—(Optional) Interface name for the SSH session. (This option does not work when default-address-selection is configured at the [edit system] hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system logical-system-name—(Optional) Name of a particular logical system for the SSH attempt.

tenant tenant-name—(Optional) Name of a particular tenant system for the SSH attempt.

routing-instance routing-instance-name—(Optional) Name of the routing instance for the SSH attempt.

source address—(Optional) Source address of the SSH connection.

v2—(Optional) Use SSH version 2 when connecting to a remote host.

port port-number—(Optional) Specify a port number for the SSH connection.

Additional Information
To configure an SSH (version 2) key for your user account, include the authentication dsa-rsa statement at the [edit system login user user-name] hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the retry-options statement at the [edit system login] hierarchy level.

Required Privilege Level
network

RELATED DOCUMENTATION
Configuring SSH Host Keys for Secure Copying of Data | 300

List of Sample Output
ssh on page 2900
Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```bash
ssh

user@switch> ssh user

Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?user' added to the list of known hosts.
user@device's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```
telnet

List of Syntax
Syntax on page 2901
Syntax (EX Series Switches) on page 2901
Syntax (Junos OS Evolved) on page 2901

Syntax

telnet host
<8bit>
<inet | inet6>
<port port-number>
<routing-instance routing-instance-name>
<logical-system logical-system-name>
<tenant tenant-name>

Syntax (EX Series Switches)

telnet host
<8bit>
<bypass-routing>
<inet | inet6>
<interface interface-name>
<no-resolve>
<port port-number>
<routing-instance routing-instance-name>
<source source-address>

Syntax (Junos OS Evolved)

telnet host
<8bit>
<inet | inet6>
<port port-number>
<routing-instance routing-instance-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
The following options are deprecated in Junos OS Evolved Release 18.3R1: bypass-routing, interface, no-resolve, and source.
The command tenant option is introduced in Junos OS Release 19.2R1 for SRX Series.

**Description**

Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type quit to exit from telnet.

**NOTE:** For Junos OS Evolved, use the routing-instance mgmt_junos option to access a remote system through the management interface.

**Options**

- **host**—Name or address of the remote system.
- **8bit**—(Optional) Use an 8-bit data path.
- **bypass-routing**—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.
- **inet | inet6**—(Optional) Open an IPv4 or IPv6 session, respectively.
- **interface interface-name**—(Optional) Interface name for the telnet session. (This option does not work when default-address-selection is configured at the [edit system] hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)
- **logical-system logical-system-name**—(Optional) Name of a particular logical system for the telnet attempt.
- **tenant tenant-name**—(Optional) Name of a particular tenant system for the telnet attempt.
- **no-resolve**—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Do not attempt to determine the hostname that corresponds to the IP address.
- **port port-number**—(Optional) Port number or service name on the remote system.
- **routing-instance routing-instance-name**—(Optional) Name of the routing instance for the telnet attempt.
- **source source-address**—(Optional) This option is not supported for Junos OS Evolved Release 18.3R1. Source address of the telnet connection.

**Additional Information**

You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the retry-options statement at the [edit system login] hierarchy level.

**Required Privilege Level**

network
List of Sample Output
telnet on page 2903

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
telnet

user@host> telnet 192.154.1.254

Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
ttypa
login:
test access profile

Syntax

```
test access profile profile-name user username password password <detail>
```

Release Information

Command introduced in Junos OS Release 9.1.

Description

Specify a profile to use to get information from a RADIUS server, which includes all the information from the `test access radius-server` command.

Options

- `detail`—(Optional) Show the RADIUS attributes returned by the server.
- `profile-name`—Access profile name configured.
- `password`—Password for the username.
- `username`—User name to be authenticated to the RADIUS server.

Required Privilege Level

`view`

List of Sample Output

- `test access profile` on page 2905
- `test access profile detail` on page 2906

Output Fields

Table 125 on page 2904 lists the output fields for the `test access profile` command. Output fields are listed in the approximate order in which they appear.

**Table 125: test access profile Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Name of the configured access profile.</td>
</tr>
<tr>
<td>Client Username</td>
<td>The user name authenticated by the RADIUS server.</td>
</tr>
<tr>
<td>Client Password</td>
<td>The user password authenticated by the RADIUS server.</td>
</tr>
<tr>
<td>Num Servers</td>
<td>Number of RADIUS servers in the configured access profile.</td>
</tr>
</tbody>
</table>
Table 125: test access profile Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server List</td>
<td>List of RADIUS servers in the configure access profile.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the RADIUS server authenticated.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>The RADIUS server port utilized during the authentication test.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The source IP address of the client making the RADIUS request. If no address is shown, it defaults to the address of the outgoing interface.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The RADIUS server timeout period.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>The number of authentication attempts allowed by the RADIUS server.</td>
</tr>
<tr>
<td>Secret</td>
<td>The shared secret used for authentication with the RADIUS server.</td>
</tr>
<tr>
<td>Status</td>
<td>The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication.</td>
</tr>
<tr>
<td>Attempts</td>
<td>The number of authentication attempts on the RADIUS server.</td>
</tr>
<tr>
<td>Attribute List</td>
<td>The list of returned RADIUS attributes, sorted by the attribute name, and including parameter length and value. See your RADIUS server documentation for attribute descriptions.</td>
</tr>
<tr>
<td>(Attribute) Name</td>
<td>The name of the attribute.</td>
</tr>
<tr>
<td>(Attribute) Length</td>
<td>The attribute length in bytes.</td>
</tr>
<tr>
<td>(Attribute) Value</td>
<td>The attribute value.</td>
</tr>
</tbody>
</table>

Sample Output

test access profile

The following example uses the **test access profile** command to access and display basic information about the RADIUS server(s) shown in the resulting output:
user@host> test access profile alpha user TEST password TEST

Test Radius Profile Access
Profile Name : alpha
Client Username : TEST
Client Password : TEST
Num Servers : 5

Server List

<table>
<thead>
<tr>
<th>Attempts</th>
<th>IP Address</th>
<th>Port</th>
<th>Source Address</th>
<th>Retry Count</th>
<th>Secret</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1.1.1.1</td>
<td>1812</td>
<td>10.10.10.10</td>
<td>2</td>
<td>1</td>
<td>TEST</td>
</tr>
<tr>
<td></td>
<td>1.2.3.4</td>
<td>1812</td>
<td>Default</td>
<td>1</td>
<td>2</td>
<td>TEST</td>
</tr>
<tr>
<td></td>
<td>192.168.10.10</td>
<td>1812</td>
<td>Default</td>
<td>3</td>
<td>3</td>
<td>TEST</td>
</tr>
</tbody>
</table>

Test access profile detail
The following example uses the test access profile detail command to access and display detailed information about the RADIUS server(s) shown in the resulting output:

user@host> test access profile alpha user TEST password TEST detail

Test Radius Profile Access Detailed
Profile Name : alpha
Client Username : TEST
Client Password : TEST
Num Servers : 5

Radius Server List

<table>
<thead>
<tr>
<th>IP Address</th>
<th>UDP Port</th>
<th>Source Address</th>
<th>Timeout</th>
<th>Retry Count</th>
<th>Secret</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>1812</td>
<td>192.168.10.10</td>
<td>2</td>
<td>1</td>
<td>TEST</td>
<td>Timeout</td>
</tr>
</tbody>
</table>

Attempts

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEST</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
</tr>
</tbody>
</table>

Attempts

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.5</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>Class</td>
</tr>
<tr>
<td>Acct-Interim-Interval</td>
</tr>
<tr>
<td>Callback-Id</td>
</tr>
<tr>
<td>Callback-Number</td>
</tr>
<tr>
<td>Class</td>
</tr>
<tr>
<td>Filter-Id</td>
</tr>
<tr>
<td>Filter-Id</td>
</tr>
<tr>
<td>Framed-Compression</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
</tr>
<tr>
<td>Framed-IPv6-Route</td>
</tr>
<tr>
<td>Framed-MTU</td>
</tr>
<tr>
<td>Framed-Pool</td>
</tr>
<tr>
<td>Framed-Protocol</td>
</tr>
<tr>
<td>Framed-Route</td>
</tr>
<tr>
<td>Framed-Routing</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Idle-Timeout</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Login-IP-Host</td>
</tr>
<tr>
<td>Login-LAT-Group</td>
</tr>
<tr>
<td>Login-LAT-Node</td>
</tr>
<tr>
<td>Login-LAT-Port</td>
</tr>
<tr>
<td>Feature</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Login-LAT-Service</td>
</tr>
<tr>
<td>Login-Service</td>
</tr>
<tr>
<td>Login-TCP-Port</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Vendor-Specific</td>
</tr>
<tr>
<td>Password-Retry</td>
</tr>
<tr>
<td>Port-Limit</td>
</tr>
<tr>
<td>Prompt</td>
</tr>
<tr>
<td>Reply-Message</td>
</tr>
<tr>
<td>Service-Type</td>
</tr>
<tr>
<td>Session-Timeout</td>
</tr>
<tr>
<td>Termination-Action</td>
</tr>
<tr>
<td>Tunnel-Assignment-ID</td>
</tr>
<tr>
<td>Tunnel-Client-Auth-ID</td>
</tr>
<tr>
<td>Tunnel-Client-Endpoint</td>
</tr>
<tr>
<td>Tunnel-Password</td>
</tr>
<tr>
<td>Tunnel-Type</td>
</tr>
<tr>
<td>MS BAP Usage</td>
</tr>
<tr>
<td>MS-CHAP MPPE-Keys</td>
</tr>
<tr>
<td>MS-CHAP2 Success</td>
</tr>
<tr>
<td>MS Filter</td>
</tr>
<tr>
<td>MS Link Drop Time Limit</td>
</tr>
<tr>
<td>MS Link Utilization Threshold</td>
</tr>
<tr>
<td>MS MPPE Encryption Policy</td>
</tr>
<tr>
<td>MS MPPE Encryption Types</td>
</tr>
<tr>
<td>MS Primary DNS Server</td>
</tr>
<tr>
<td>MS Primary NBNS Server</td>
</tr>
<tr>
<td>MS Secondary DNS Server</td>
</tr>
<tr>
<td>MS Secondary NBNS Server</td>
</tr>
</tbody>
</table>
test access radius-server

Syntax

test access radius-server address user username password password secret secret
<authentication-port port>
<retry number>
<source-address address>
<timeout number>

Release Information
Command introduced in Junos OS Release 9.1.

Description
Verify RADIUS server authentication parameters.

Options
address—RADIUS server under test IP address.

password—Password for the user.

secret—Secret shared with the RADIUS server.

user—User name to be authenticated to the RADIUS server.

authentication-port—(Optional) RADIUS server authentication port number (1through 65535).

retry—(Optional) Retry attempts (1through 10).

source-address—(Optional) Use an alternate address as the source address.

timeout—(Optional) Request timeout period (1through 90 seconds).

Required Privilege Level
view

List of Sample Output
test access radius-server user password secret on page 2910

Output Fields
Table 126 on page 2910 lists the output fields for the test access radius-server command. Output fields are listed in the approximate order in which they appear.
### Table 126: test access radius-server Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The IP address of the RADIUS server authenticated.</td>
</tr>
<tr>
<td>UDP port</td>
<td>The RADIUS server port utilized during the authentication test.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>&quot;Default&quot; is shown if the IP address is the same as that of the RADIUS server. Alternatively, an IP address specified for authentication is shown.</td>
</tr>
<tr>
<td>Server timeout</td>
<td>The RADIUS server timeout period.</td>
</tr>
<tr>
<td>Sever retry count</td>
<td>The number of authentication attempts allowed by the RADIUS server.</td>
</tr>
<tr>
<td>Secret</td>
<td>The shared secret used for authentication with the RADIUS server.</td>
</tr>
<tr>
<td>Client Username</td>
<td>The user name authenticated by the RADIUS server.</td>
</tr>
<tr>
<td>Client Password</td>
<td>The user password authenticated by the RADIUS server.</td>
</tr>
<tr>
<td>Status</td>
<td>The test result status (Accepted or Rejected) and the number of retransmits utilized during authentication.</td>
</tr>
</tbody>
</table>

### Sample Output

**test access radius-server user password secret**

The following example command tests RADIUS authentication with a specific server (172.28.30.95), user (JOHNDOE), secret (No1Knows), and password (JohnPass); and displays the resulting output:

```bash
user@host> test access radius-server 172.28.30.95 user JOHNDOE password JohnPass secret No1Knows
```

#### Test Radius Server Access

- **Server**: 172.28.30.95
- **UDP port**: 1812
- **Source IP Address**: Default
- **Server timeout**: 3
- **Sever retry count**: 3
<table>
<thead>
<tr>
<th>Secret</th>
<th>: No1Knows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Username</td>
<td>: JOHNDOE</td>
</tr>
<tr>
<td>Client Password</td>
<td>: JohnPass</td>
</tr>
<tr>
<td>Status</td>
<td>: Accepted, retransmits: 0</td>
</tr>
</tbody>
</table>