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 Interfaces Fundamentals for Routing Devices
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/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
# Table of Contents

About the Documentation ....................................................... xli
  Documentation and Release Notes ......................................... xli
  Using the Examples in This Manual ....................................... xli
    Merging a Full Example ................................................ xli
    Merging a Snippet .................................................... xlii
  Documentation Conventions ................................................. xliii
  Documentation Feedback .................................................. xliv
  Requesting Technical Support ............................................. xlv
  Self-Help Online Tools and Resources .................................... xlvi
  Creating a Service Request with JTAC ................................. xlvi

## Part 1

### Chapter 1

**Router Interfaces** .......................................................... 3

**Router Interfaces Overview** ............................................. 4

**Types of Interfaces Overview** .......................................... 4

**Understanding Permanent Interfaces** ................................... 5

**Understanding Transient Interfaces** ................................... 5

**Understanding Services Interfaces** ..................................... 7

**Understanding Container Interfaces** .................................... 8
  
  **Understanding Traditional APS Concept** .............................. 8
  **Container Interfaces Concept** ......................................... 9
  **APS Support for Container-Based Interfaces** .......................... 9
  **Autocopy of APS Parameters** .......................................... 9

**Understanding Management Ethernet Interfaces**........................ 10

**Understanding Interfaces on ACX Series Universal Metro Routers** .... 10

  **T1 and E1 Time-Division Multiplexing (TDM) Interfaces** .......... 11
  **Inverse Multiplexing for ATM (IMA)** ................................ 12
  **Gigabit Ethernet interfaces** ....................................... 12

**TX Matrix Plus and T1600 Router (Routing Matrix) Management Ethernet Interfaces** ........................................ 13

**Understanding Internal Ethernet Interfaces** ........................... 14

**T1600 Routers (Routing Matrix) Internal Ethernet Interfaces** ....... 16

**Interface Naming Overview** ............................................. 16

  **Physical Part of an Interface Name** ................................... 17
  **Logical Part of an Interface Name** .................................. 23
  **Separators in an Interface Name** .................................... 23
  **Channel Part of an Interface Name** .................................. 23

**Interface Naming for a Routing Matrix Based on a TX Matrix Router** ................................................. 24

**Interface Naming for a Routing Matrix Based on a TX Matrix Plus Router** .................................................. 26

**Chassis Interface Naming** ............................................... 28
Unicast RPF with Routing Asymmetry ........................................ 229
Configuring Unicast RPF Strict Mode .................................... 229
Configuring Unicast RPF Loose Mode ................................... 231
Configuring Unicast RPF Loose Mode with Ability to Discard Packets .... 233
Configuring Unicast RPF on a VPN ............................................ 234
Configuring Unicast RPF ......................................................... 235
Understanding and Preventing Unknown Unicast Forwarding .................... 236
Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface .................................................. 236
Configuring Unknown Unicast Forwarding (ELS) ................................. 237
Configuring Unknown Unicast Forwarding on EX4300 Switches .................. 238
Configuring Unknown Unicast Forwarding on EX9200 Switches .................. 238
Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface .................................................. 240
Configuring Unknown Unicast Forwarding (CLI Procedure) ...................... 241
Enabling Source Class and Destination Class Usage .................................. 241
Source Class and Destination Class Usage .................................... 241
Enabling Source Class and Destination Class Usage .................................. 245
Understanding Targeted Broadcast ............................................. 250
Configuring Targeted Broadcast .............................................. 251
Configuring Targeted Broadcast and Its Options .................................. 251
Display Targeted Broadcast Configuration Options ............................... 252
Forward IP Packets On the Egress Interface and To the Routing Engine ........................... 253
Forward IP Packets On the Egress Interface Only .................................. 253

Chapter 5 Configuring Circuit and Translational Cross-Connects ............ 255
Circuit and Translational Cross-Connects Overview .............................. 255
Defining the Encapsulation for Switching Cross-Connects ...................... 257
Defining the Encapsulation for Switching Cross-Connects ...................... 258
Configuring PPP or Cisco HDLC Circuits ..................................... 258
Configuring ATM Circuits ...................................................... 258
Configuring Frame Relay Circuits .............................................. 259
Configuring Ethernet CCC Circuits ............................................ 260
Configuring Ethernet VLAN Circuits .......................................... 260
Defining the Connection for Switching Cross-Connects ............................ 261
Configuring MPLS for Switching Cross-Connects .................................. 261
Configuring IS-IS or MPLS Traffic for TCC Interfaces ......................... 262
Configuring ATM-to-Ethernet Interworking ...................................... 262
ATM-to-Ethernet Interworking ................................................. 263
Enabling ATM-to-Ethernet Interworking ...................................... 263
Configuring the Ethernet Interface ............................................. 264
Configuring Ethernet Encapsulation .......................................... 264
Configuring the Outer VLAN Identifier ...................................... 264
Configuring the Inner VLAN Identifier Range .................................. 264
Configuring the Physical Interface VPI ...................................... 265
Configuring the ATM Logical Interface ...................................... 265
Configuring the Protocol Family ............................................... 265
Configuring the Logical Interface VPI ...................................... 266
### Table of Contents

- Configuring the Logical Interface VCI ........................................ 266
- ATM-To-Ethernet Interworking on ATM MICs ............................... 267
  - Limitations ............................................................................. 267
- Example: Configuring a CCC over Frame Relay Encapsulated Interface ... 268
- Example: Configuring a TCC ....................................................... 269
- Example: Configuring CCC over Aggregated Ethernet .................... 270
- Example: Configuring a Remote LSP CCC over Aggregated Ethernet ... 272
- Example: Configuring ATM-to-Ethernet Interworking .................... 274
- Example: Configuring ATM-to-Ethernet Interworking on ATM MIC .... 275
- Verifying ATM-to-Ethernet Interworking Configuration on ATM MICs ... 281
  - Verifying That The ATM Interface on Router1 Is Configured Correctly ... 281
  - Verifying The Status of the MIC on Router1 ............................... 282
  - Verify That OSPF Configuration on Router1 Is Accurate ................ 282
  - Verify That LDP Configuration on Router1 Is Accurate .................. 283
  - Verify That Layer 2 Virtual Circuit Session Configuration on Router1 Is Accurate .............................................. 283
  - Verifying That the Ethernet Interface on Router2 Is Configured Correctly ... 284
  - Verifying the Status of the MIC on Router2 ............................... 284
  - Verify That OSPF Configuration on Router2 Is Accurate ................. 284
  - Verify That LDP Configuration on Router2 Is Accurate ................. 285
  - Verify That Layer 2 Virtual Circuit Session Configuration on Router2 Is Accurate .............................................. 285

### Part 2 Special Router Interfaces

#### Chapter 6 Configuring Discard Interfaces ............................. 289
- Discard Interfaces Overview .................................................... 289
- Understanding Discard Interfaces ............................................. 289
- Guidelines to Follow When Configuring a Discard Interface .......... 289
- Configuring Discard Interfaces ............................................... 290
- Configuring and Usage of Discard Interface .............................. 290
- Configure an Output Filter with Output policy ........................... 291

#### Chapter 7 Configuring IP Demultiplexing Interfaces ............... 293
- Demultiplexing Interface Overview .......................................... 293
- IP Demux Interface Overview ............................................... 293
- VLAN Demux Interface Overview ......................................... 294
- Guidelines to Remember When Configuring A Demux Interface ...... 294
  - Points to Remember When Configuring an IP Demux Interface ...... 295
  - Points to Remember When Configuring a VLAN Demux Interface ... 295
- MAC Address Validation on Static Demux Interfaces .................. 295
  - Loose .................................................................................... 295
  - Strict ...................................................................................... 296
- Configuring an IP Demultiplexing Interface ................................ 296
- Configuring an IP Demux Underlying Interface .......................... 297
- Configuring the IP Demux Interface ....................................... 298
- Configuring MAC Address Validation on Static IP Demux Interfaces ... 300
- Configuring a VLAN Demultiplexing Interface ............................ 301
- Configuring a VLAN Demux Underlying Interface ...................... 301
- Configuring the VLAN Demux Interface .................................. 303
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring MAC Address Validation on Static VLAN Demux Interfaces</td>
<td>305</td>
</tr>
<tr>
<td>Verifying a Demux Interface Configuration</td>
<td>306</td>
</tr>
<tr>
<td>Chapter 8</td>
<td></td>
</tr>
<tr>
<td>Configuring the Loopback Interface</td>
<td>309</td>
</tr>
<tr>
<td>Understanding the Loopback Interface</td>
<td>309</td>
</tr>
<tr>
<td>Loopback Interface Configuration</td>
<td>310</td>
</tr>
<tr>
<td>Configuring the Loopback Interface</td>
<td>310</td>
</tr>
<tr>
<td>Example: Configuring Two Addresses on the Loopback Interface with Host</td>
<td>311</td>
</tr>
<tr>
<td>Routes</td>
<td></td>
</tr>
<tr>
<td>Example: Configuring Two Addresses on the Loopback Interface with</td>
<td>311</td>
</tr>
<tr>
<td>Subnetwork Routes</td>
<td></td>
</tr>
<tr>
<td>Example: Configuring an IPv4 and an IPv6 Address on the Loopback</td>
<td>312</td>
</tr>
<tr>
<td>Interface with Subnetwork Routes</td>
<td></td>
</tr>
<tr>
<td>Part 3</td>
<td></td>
</tr>
<tr>
<td>Serial Interfaces</td>
<td></td>
</tr>
<tr>
<td>Chapter 9</td>
<td></td>
</tr>
<tr>
<td>Serial Interfaces Overview</td>
<td>315</td>
</tr>
<tr>
<td>Chapter 10</td>
<td></td>
</tr>
<tr>
<td>Configuring Serial Interfaces</td>
<td>317</td>
</tr>
<tr>
<td>Example: Physical Interface Configuration Statements for Serial</td>
<td>317</td>
</tr>
<tr>
<td>Interfaces</td>
<td></td>
</tr>
<tr>
<td>Configuring the Serial Line Protocol</td>
<td>318</td>
</tr>
<tr>
<td>Configuring the Serial Line Protocol</td>
<td>318</td>
</tr>
<tr>
<td>Serial Interface Default Settings</td>
<td>318</td>
</tr>
<tr>
<td>Serial Interface Default Settings</td>
<td>319</td>
</tr>
<tr>
<td>Invalid Serial Interface Statements</td>
<td>320</td>
</tr>
<tr>
<td>Configuring the Serial Clocking Mode</td>
<td>322</td>
</tr>
<tr>
<td>Configuring the Serial Clocking Mode</td>
<td>322</td>
</tr>
<tr>
<td>Inverting the Serial Interface Transmit Clock</td>
<td>323</td>
</tr>
<tr>
<td>Configuring the DTE Clock Rate</td>
<td>323</td>
</tr>
<tr>
<td>Configuring the Serial Signal Handling</td>
<td>324</td>
</tr>
<tr>
<td>Configuring the Serial DTR Circuit</td>
<td>327</td>
</tr>
<tr>
<td>Configuring Serial Signal Polarities</td>
<td>327</td>
</tr>
<tr>
<td>Configuring Serial Loopback Capability</td>
<td>328</td>
</tr>
<tr>
<td>Configuring Serial Line Encoding</td>
<td>330</td>
</tr>
<tr>
<td>Specifying a USB Modem Interface on J Series Routers</td>
<td>331</td>
</tr>
<tr>
<td>Part 4</td>
<td></td>
</tr>
<tr>
<td>Monitoring and Troubleshooting Interfaces</td>
<td></td>
</tr>
<tr>
<td>Chapter 11</td>
<td></td>
</tr>
<tr>
<td>Monitoring Interfaces</td>
<td>335</td>
</tr>
<tr>
<td>Tracing Interface Operations Overview</td>
<td>335</td>
</tr>
<tr>
<td>Tracing Operations of an Individual Router Interface</td>
<td>335</td>
</tr>
<tr>
<td>Tracing Operations of the Interface Process</td>
<td>336</td>
</tr>
<tr>
<td>Monitoring a PPP Session</td>
<td>338</td>
</tr>
<tr>
<td>Tracing Operations of the pppd Process</td>
<td>338</td>
</tr>
<tr>
<td>Chapter 12</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Interfaces</td>
<td>341</td>
</tr>
<tr>
<td>Configuring Interface Diagnostics Tools to Test the Physical Layer</td>
<td></td>
</tr>
<tr>
<td>Connections</td>
<td>341</td>
</tr>
<tr>
<td>Configuring Loopback Testing</td>
<td>341</td>
</tr>
<tr>
<td>Configuring BERT Testing</td>
<td>343</td>
</tr>
</tbody>
</table>
Part 5 Configuration Statements and Operational Commands

Chapter 13 Configuration Statements ........................................ 369

802.3ad .......................................................... 388
accept .......................................................... 389
accept-source-mac .................................................. 391
access-concentrator .................................................. 393
access-profile ...................................................... 394
accounting ......................................................... 395
accounting-profile .................................................. 396
acfc ............................................................... 397
acknowledge-retries .................................................. 398
acknowledge-timer .................................................... 399
action (OAM) ..................................................... 400
action (Policer) ...................................................... 400
action-profile (Applying to CFM) .................................. 401
action-profile (Defining for CFM) .................................. 402
action-profile ....................................................... 403
action-red-differential-delay ....................................... 404
activation-delay ..................................................... 405
activation-priority .................................................... 406
address .......................................................... 407
advertise-interval .................................................... 409
age ................................................................. 410
agent-specifier ....................................................... 411
aggregate (Gigabit Ethernet CoS Policer) ......................... 412
aggregate (Hierarchical Policer) .................................... 413
aggregate (SONET/SDH) .......................................... 414
aggregate-ports ..................................................... 414
aggregated-ether-options .......................................... 415
aggregated-sonet-options .......................................... 416
alarm (optics-options) .............................................. 417
alias (Interfaces) ................................................... 418
allow-any-vci ....................................................... 419
allow-fragmentation .................................................. 420
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>clocking</td>
<td>472</td>
</tr>
<tr>
<td>clocking-mode</td>
<td>473</td>
</tr>
<tr>
<td>community (Policy Options)</td>
<td>474</td>
</tr>
<tr>
<td>compatibility-mode</td>
<td>477</td>
</tr>
<tr>
<td>compression (PPP Properties)</td>
<td>478</td>
</tr>
<tr>
<td>compression (Voice Services)</td>
<td>479</td>
</tr>
<tr>
<td>compression-device</td>
<td>480</td>
</tr>
<tr>
<td>connections</td>
<td>480</td>
</tr>
<tr>
<td>connection-protection-tlv</td>
<td>481</td>
</tr>
<tr>
<td>connectivity-fault-management</td>
<td>482</td>
</tr>
<tr>
<td>container-devices</td>
<td>483</td>
</tr>
<tr>
<td>container-list</td>
<td>484</td>
</tr>
<tr>
<td>container-options</td>
<td>485</td>
</tr>
<tr>
<td>container-type</td>
<td>486</td>
</tr>
<tr>
<td>continuity-check</td>
<td>487</td>
</tr>
<tr>
<td>control-channel</td>
<td>488</td>
</tr>
<tr>
<td>control-polarity</td>
<td>489</td>
</tr>
<tr>
<td>control-signal</td>
<td>490</td>
</tr>
<tr>
<td>copy-tos-to-outer-ip-header</td>
<td>491</td>
</tr>
<tr>
<td>core-dump</td>
<td>492</td>
</tr>
<tr>
<td>crc-major-alarm-threshold</td>
<td>493</td>
</tr>
<tr>
<td>crc-minor-alarm-threshold</td>
<td>494</td>
</tr>
<tr>
<td>cts</td>
<td>495</td>
</tr>
<tr>
<td>cts-polarity</td>
<td>496</td>
</tr>
<tr>
<td>cycle-time</td>
<td>497</td>
</tr>
<tr>
<td>damping (Interfaces)</td>
<td>498</td>
</tr>
<tr>
<td>data-channel</td>
<td>500</td>
</tr>
<tr>
<td>data-tlv-size</td>
<td>501</td>
</tr>
<tr>
<td>dcd</td>
<td>502</td>
</tr>
<tr>
<td>dcd-polarity</td>
<td>503</td>
</tr>
<tr>
<td>dce</td>
<td>503</td>
</tr>
<tr>
<td>deactivation-delay</td>
<td>504</td>
</tr>
<tr>
<td>dce-options</td>
<td>505</td>
</tr>
<tr>
<td>default-actions</td>
<td>506</td>
</tr>
<tr>
<td>default-chap-secret</td>
<td>507</td>
</tr>
<tr>
<td>default-pap-password</td>
<td>508</td>
</tr>
<tr>
<td>delimiter</td>
<td>508</td>
</tr>
<tr>
<td>demux-destination (Underlying Interface)</td>
<td>509</td>
</tr>
<tr>
<td>demux-destination (Demux Interface)</td>
<td>510</td>
</tr>
<tr>
<td>demux-options (Static Interface)</td>
<td>511</td>
</tr>
<tr>
<td>demux-source (Demux Interface)</td>
<td>512</td>
</tr>
<tr>
<td>demux-source (Underlying Interface)</td>
<td>513</td>
</tr>
<tr>
<td>demux0 (Static Interface)</td>
<td>514</td>
</tr>
<tr>
<td>demux0 (Dynamic Interface)</td>
<td>515</td>
</tr>
<tr>
<td>description (Interfaces)</td>
<td>516</td>
</tr>
<tr>
<td>destination (IPCP)</td>
<td>517</td>
</tr>
<tr>
<td>destination (Routing Instance)</td>
<td>518</td>
</tr>
<tr>
<td>destination (Tunnels)</td>
<td>519</td>
</tr>
<tr>
<td>destination-class-usage</td>
<td>520</td>
</tr>
<tr>
<td>delimiter</td>
<td>521</td>
</tr>
</tbody>
</table>
# Table of Contents

- event (LFM) ................................................................. 596
- event-thresholds .................................................. 597
- fast-aps-switch .................................................... 598
- f-max-period ....................................................... 599
- facility-override .................................................. 599
- failover-delay ..................................................... 600
- family (Dynamic Standard Interface) .......................... 601
- family ................................................................. 603
- fastether-options .................................................. 609
- fcs ..................................................................... 610
- feac-loop-respond ................................................. 611
- fec (gigether) ....................................................... 612
- filter ................................................................. 614
- filter (Applying to an Interface) ................................. 616
- flexible-vlan-tagging .............................................. 617
- flow-control ....................................................... 618
- flow-control-options .............................................. 619
- force ................................................................. 620
- forward-and-send-to-re ........................................... 621
- forwarding-class (ATM2 IQ Scheduler Maps) ................. 622
- forwarding-class (Gigabit Ethernet IQ Classifier) .......... 623
- forward-only ....................................................... 624
- fragment-threshold ................................................ 625
- frame-error ........................................................ 626
- frame-period ....................................................... 627
- frame-period-summary ............................................ 628
- framing (E1, E3, and T1 Interfaces) ............................ 629
- framing (10-Gigabit Ethernet Interfaces) ....................... 630
- framing (SONET and SDH Interfaces) ........................... 631
- gigether-options ................................................... 632
- gratuitous-arp-reply .............................................. 634
- guard-interval ..................................................... 635
- hardware-assisted-timestamping ................................ 636
- high-plp-threshold ................................................. 637
- hello-timer ........................................................ 638
- hierarchical-policer .............................................. 639
- hierarchical-scheduler (Subscriber Interfaces on MX Series Routers) ........................................... 640
- high-plp-max-threshold .......................................... 641
- high-plp-threshold ................................................. 642
- hold-interval (OAM) ............................................... 643
- hold-interval (Protection Group) ................................ 644
- hold-time (APS) ..................................................... 645
- hold-time (Physical Interface) .................................... 646
- hold-time (SONET/SDH Defect Triggers) ......................... 648
- host (Interfaces) .................................................... 649
- host-prefix-only ................................................... 650
- iccp ................................................................. 651
- idle-cycle-flag ..................................................... 653
- idle-timeout ....................................................... 654
ncp-restart-timer ......................................................... 816
nd6-stale-time ......................................................... 817
negotiate-address ..................................................... 818
negotiation-options .................................................. 819
neighbor (Automatic Protection Switching for SONET/SDH) ........ 820
no-allow-link-events .................................................. 820
no-aggregate-delegate-processing ................................. 821
asynchronous-notification ......................................... 822
no-auto-mdix .......................................................... 823
auto-negotiation ....................................................... 824
cbit-parity ............................................................. 826
core-dump .................................................................. 827
feac-loop-respond ...................................................... 828
flow-control .............................................................. 829
gratuitous-arp-reply .................................................... 830
no-gratuitous-arp-request .......................................... 831
no-keepalives ........................................................... 832
long-buildout ............................................................ 833
loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet) .. 834
mac-learn-enable ....................................................... 835
no-partition ............................................................... 836
payload-scrambler ..................................................... 838
no-pre-classifier ....................................................... 839
no-redirects ............................................................. 840
source-filtering .......................................................... 841
syslog (Monitoring) ..................................................... 842
no-termination-request .............................................. 843
translate-discard-eligible .......................................... 844
translate-fecn-and-becn ............................................. 844
unframed ................................................................ 845
z0-increment ............................................................. 845
node-id ................................................................. 846
non-revertive (Interfaces) ............................................ 846
oam ................................................................. 847
oam-liveness ............................................................ 850
oam-period .............................................................. 851
oc-slice ............................................................... 852
open-timeout ............................................................ 853
operating-mode ........................................................ 854
optics-options .......................................................... 855
option-82 ............................................................... 856
otn-options ............................................................. 857
output ................................................................. 859
output-list ............................................................... 860
output-policer .......................................................... 861
output-priority-map ................................................... 862
output-three-color ..................................................... 863
output-vlan-map (Aggregated Ethernet) ........................... 864
output-vlan-map ........................................................ 865
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>overflow (Receive Bucket)</td>
<td>866</td>
</tr>
<tr>
<td>overflow (Transmit Bucket)</td>
<td>866</td>
</tr>
<tr>
<td>override</td>
<td>867</td>
</tr>
<tr>
<td>pado-advertise</td>
<td>868</td>
</tr>
<tr>
<td>paired-group</td>
<td>869</td>
</tr>
<tr>
<td>pap</td>
<td>870</td>
</tr>
<tr>
<td>partition</td>
<td>871</td>
</tr>
<tr>
<td>passive (CHAP)</td>
<td>872</td>
</tr>
<tr>
<td>passive (PAP)</td>
<td>873</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>874</td>
</tr>
<tr>
<td>password (Interfaces)</td>
<td>875</td>
</tr>
<tr>
<td>path-database-size</td>
<td>875</td>
</tr>
<tr>
<td>path-trace</td>
<td>876</td>
</tr>
<tr>
<td>payload-scrambler</td>
<td>877</td>
</tr>
<tr>
<td>payload-size</td>
<td>878</td>
</tr>
<tr>
<td>pdu-interval</td>
<td>879</td>
</tr>
<tr>
<td>pdu-threshold</td>
<td>880</td>
</tr>
<tr>
<td>peer</td>
<td>881</td>
</tr>
<tr>
<td>peer-unit</td>
<td>882</td>
</tr>
<tr>
<td>per-unit-scheduler</td>
<td>883</td>
</tr>
<tr>
<td>performance-monitoring</td>
<td>885</td>
</tr>
<tr>
<td>periodic</td>
<td>886</td>
</tr>
<tr>
<td>pfc</td>
<td>887</td>
</tr>
<tr>
<td>pic-type</td>
<td>887</td>
</tr>
<tr>
<td>plp-to-clp</td>
<td>888</td>
</tr>
<tr>
<td>plp1</td>
<td>889</td>
</tr>
<tr>
<td>point-to-point</td>
<td>890</td>
</tr>
<tr>
<td>policer (CFM Firewall)</td>
<td>891</td>
</tr>
<tr>
<td>policer (CFM Global)</td>
<td>892</td>
</tr>
<tr>
<td>policer (CFM Session)</td>
<td>893</td>
</tr>
<tr>
<td>policer (CoS)</td>
<td>894</td>
</tr>
<tr>
<td>policer (Interface)</td>
<td>895</td>
</tr>
<tr>
<td>policer (MAC)</td>
<td>896</td>
</tr>
<tr>
<td>policy-statement</td>
<td>897</td>
</tr>
<tr>
<td>pool</td>
<td>901</td>
</tr>
<tr>
<td>pop</td>
<td>902</td>
</tr>
<tr>
<td>pop-all-labels</td>
<td>903</td>
</tr>
<tr>
<td>pop-pop</td>
<td>904</td>
</tr>
<tr>
<td>pop-swap</td>
<td>905</td>
</tr>
<tr>
<td>port</td>
<td>906</td>
</tr>
<tr>
<td>port-priority</td>
<td>907</td>
</tr>
<tr>
<td>port-status-tlv</td>
<td>908</td>
</tr>
<tr>
<td>post-service-filter</td>
<td>909</td>
</tr>
<tr>
<td>ppp-options</td>
<td>910</td>
</tr>
<tr>
<td>pppoe-options</td>
<td>912</td>
</tr>
<tr>
<td>pppoe-underlying-options (Static and Dynamic Subscribers)</td>
<td>913</td>
</tr>
<tr>
<td>preferred</td>
<td>914</td>
</tr>
<tr>
<td>preferred-source-address</td>
<td>915</td>
</tr>
<tr>
<td>preferred-source-address</td>
<td>916</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>1019</td>
</tr>
<tr>
<td>start-end-flag</td>
<td>1020</td>
</tr>
<tr>
<td>static-interface</td>
<td>1021</td>
</tr>
<tr>
<td>static-tei-val</td>
<td>1022</td>
</tr>
<tr>
<td>supplicant</td>
<td>1023</td>
</tr>
<tr>
<td>supplicant-timeout</td>
<td>1024</td>
</tr>
<tr>
<td>swap</td>
<td>1025</td>
</tr>
<tr>
<td>swap-push</td>
<td>1026</td>
</tr>
<tr>
<td>swap-swap</td>
<td>1027</td>
</tr>
<tr>
<td>switch-options</td>
<td>1028</td>
</tr>
<tr>
<td>switch-port</td>
<td>1029</td>
</tr>
<tr>
<td>switch-type</td>
<td>1030</td>
</tr>
<tr>
<td>switching-mode</td>
<td>1031</td>
</tr>
<tr>
<td>symbol-period</td>
<td>1032</td>
</tr>
<tr>
<td>syslog (Interfaces)</td>
<td>1033</td>
</tr>
<tr>
<td>syslog (Monitoring)</td>
<td>1034</td>
</tr>
<tr>
<td>syslog (OAM Action)</td>
<td>1035</td>
</tr>
<tr>
<td>system-priority</td>
<td>1036</td>
</tr>
<tr>
<td>t1-options</td>
<td>1037</td>
</tr>
<tr>
<td>t310</td>
<td>1038</td>
</tr>
<tr>
<td>t391</td>
<td>1039</td>
</tr>
<tr>
<td>t392</td>
<td>1040</td>
</tr>
<tr>
<td>t3-4-options</td>
<td>1041</td>
</tr>
<tr>
<td>tag-protocol-id (TPIDs Expected to Be Sent or Received)</td>
<td>1042</td>
</tr>
<tr>
<td>tag-protocol-id (TPID to Rewrite)</td>
<td>1043</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>1044</td>
</tr>
<tr>
<td>targeted-distribution (Static Interfaces over Aggregated Ethernet)</td>
<td>1045</td>
</tr>
<tr>
<td>tei-option</td>
<td>1046</td>
</tr>
<tr>
<td>terminate (PPPoE Service Name Tables)</td>
<td>1047</td>
</tr>
<tr>
<td>then</td>
<td>1048</td>
</tr>
<tr>
<td>threshold</td>
<td>1049</td>
</tr>
<tr>
<td>timeslots</td>
<td>1050</td>
</tr>
<tr>
<td>tm</td>
<td>1051</td>
</tr>
<tr>
<td>tm-polarity</td>
<td>1052</td>
</tr>
<tr>
<td>traceoptions (Individual Interfaces)</td>
<td>1053</td>
</tr>
<tr>
<td>traceoptions (LACP)</td>
<td>1054</td>
</tr>
<tr>
<td>traceoptions (PPPoE)</td>
<td>1055</td>
</tr>
<tr>
<td>translate-discard-eligible</td>
<td>1056</td>
</tr>
<tr>
<td>translate-fecn-and-becn</td>
<td>1057</td>
</tr>
<tr>
<td>translate-pip-control-word-de</td>
<td>1058</td>
</tr>
<tr>
<td>transmit-bucket</td>
<td>1059</td>
</tr>
<tr>
<td>transmit-clock</td>
<td>1060</td>
</tr>
<tr>
<td>transmit-period</td>
<td>1061</td>
</tr>
<tr>
<td>transmit-weight (ATM2 IQ CoS Forwarding Class)</td>
<td>1062</td>
</tr>
<tr>
<td>transmit-weight (ATM2 IQ Virtual Circuit)</td>
<td>1063</td>
</tr>
<tr>
<td>traps</td>
<td>1064</td>
</tr>
<tr>
<td>trigger</td>
<td>1065</td>
</tr>
</tbody>
</table>
### Chapter 14 Interface Operational Commands

| Common Output Fields Description | 1152 |
| Damping Field | 1152 |
| Destination Class Field | 1152 |
| Enabled Field | 1153 |
| Filters Field | 1153 |
| Flags Fields | 1153 |
| Addresses, Flags Field | 1154 |
| Device Flags Field | 1154 |
| Family Flags Field | 1155 |
| Interface Flags Field | 1156 |
| Link Flags Field | 1156 |
| Logical Interface Flags Field | 1157 |
| Label-Switched Interface Traffic Statistics Field | 1157 |
| Policer Field | 1158 |
| Protocol Field | 1158 |
| RPF Failures Field | 1159 |
| Source Class Field | 1159 |

**Improvements to Interface Transmit Statistics Reporting** | 1160

*show interfaces* | 1161
*show interfaces (ATM)* | 1244
*show interfaces (Channelized DS3-to-DS0)* | 1280
*show interfaces (Channelized DS3-to-DS1)* | 1291
*show interfaces (Channelized E1 IQ)* | 1294
*show interfaces (Channelized E1)* | 1298
*show interfaces (Channelized OC12 IQ and IQE)* | 1309
*show interfaces (Channelized OC12)* | 1313
*show interfaces (Channelized OC3 IQ and IQE)* | 1317
*show interfaces (Channelized STMI IQ)* | 1336
*show interfaces (Channelized STMI)* | 1340
*show interfaces (Channelized T1 IQ)* | 1355
*show interfaces (Channelized T3 IQ)* | 1368
*show interfaces (Discard)* | 1370
*show interfaces (Fast Ethernet)* | 1376
*show interfaces* | 1393
*show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)* | 1476
*show interfaces (PPPoE)* | 1493
*show interfaces (PTX Series Packet Transport Routers)* | 1503
*show interfaces (SONET/SDH)* | 1519
*show interfaces (Serial)* | 1547
*show interfaces (T1, E1, or DS)* | 1560
*show interfaces (T3 or E3)* | 1585
*show interfaces demux0 (Demux Interfaces)* | 1603
*show interfaces extensive* | 1613
*show interfaces lsi (Label-Switched Interface)* | 1658
*show interfaces media* | 1661
*show interfaces terse* | 1665
## Chapter 15: ANCP Operational Commands

- clear ancp neighbor .......................................................... 1670
- clear ancp statistics ......................................................... 1672
- clear ancp subscriber ....................................................... 1675
- request ancp oam interface ............................................... 1677
- request ancp oam neighbor ............................................... 1679
- show ancp cos ............................................................... 1681
- show ancp neighbor ......................................................... 1686
- show ancp statistics ......................................................... 1694
- show ancp subscriber ....................................................... 1699
- show ancp summary ......................................................... 1706
- show ancp summary neighbor ............................................ 1708
- show ancp summary subscriber .......................................... 1710

## Chapter 16: BFD Operational Commands

- clear bfd adaptation .......................................................... 1714
- clear bfd session ............................................................. 1715
- show bfd session ............................................................. 1717

## Chapter 17: BGP Operational Commands

- clear bgp damping ............................................................ 1730
- clear bgp neighbor ........................................................... 1731
- clear bgp table ............................................................... 1734
- show bgp bmp ................................................................. 1736
- show bgp group ............................................................... 1737
- show bgp group traffic-statistics ........................................ 1745
- show bgp neighbor ........................................................... 1748
- show bgp replication ........................................................ 1768
- show bgp summary ........................................................... 1771
- show policy damping ........................................................ 1777

## Chapter 18: ES-IS Operational Commands

- clear esis adjacency ......................................................... 1780
- clear esis statistics .......................................................... 1781
- show esis adjacency ........................................................ 1782
- show esis interface .......................................................... 1785
- show esis statistics .......................................................... 1787

## Chapter 19: IP Multicast Operational Commands

- clear amt statistics .......................................................... 1792
- clear amt tunnel .............................................................. 1793
- clear igmp membership ..................................................... 1795
- clear igmp snooping membership ........................................ 1798
- clear igmp snooping statistics ............................................. 1800
- clear igmp statistics ........................................................ 1801
- clear mld membership ...................................................... 1803
- clear mld statistics .......................................................... 1804
- clear msdp cache ............................................................. 1805
- clear msdp statistics ......................................................... 1806
- clear multicast bandwidth-admission ................................. 1807
<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>IPv6 Operational Commands</th>
<th>2035</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear ipv6 neighbors</td>
<td>2036</td>
</tr>
<tr>
<td></td>
<td>clear ipv6 router-advertisement</td>
<td>2038</td>
</tr>
<tr>
<td></td>
<td>show ipv6 neighbors</td>
<td>2039</td>
</tr>
<tr>
<td></td>
<td>show ipv6 router-advertisement</td>
<td>2042</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21</th>
<th>IS-IS Operational Commands</th>
<th>2045</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear isis adjacency</td>
<td>2046</td>
</tr>
<tr>
<td></td>
<td>clear isis database</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td>clear isis overload</td>
<td>2050</td>
</tr>
<tr>
<td></td>
<td>clear isis statistics</td>
<td>2052</td>
</tr>
<tr>
<td></td>
<td>show isis adjacency</td>
<td>2054</td>
</tr>
<tr>
<td></td>
<td>show isis authentication</td>
<td>2059</td>
</tr>
<tr>
<td></td>
<td>show isis backup coverage</td>
<td>2061</td>
</tr>
<tr>
<td></td>
<td>show isis backup label-switched-path</td>
<td>2063</td>
</tr>
<tr>
<td></td>
<td>show isis backup spf results</td>
<td>2065</td>
</tr>
<tr>
<td></td>
<td>show isis context-identifier</td>
<td>2069</td>
</tr>
<tr>
<td></td>
<td>show isis database</td>
<td>2071</td>
</tr>
<tr>
<td></td>
<td>show isis hostname</td>
<td>2085</td>
</tr>
<tr>
<td></td>
<td>show isis interface</td>
<td>2087</td>
</tr>
<tr>
<td></td>
<td>show isis overview</td>
<td>2092</td>
</tr>
<tr>
<td></td>
<td>show isis route</td>
<td>2097</td>
</tr>
<tr>
<td></td>
<td>show isis spf</td>
<td>2102</td>
</tr>
<tr>
<td></td>
<td>show isis statistics</td>
<td>2107</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 22</th>
<th>LLDP Operational Commands</th>
<th>2111</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear lldp neighbors</td>
<td>2112</td>
</tr>
<tr>
<td></td>
<td>clear lldp statistics</td>
<td>2113</td>
</tr>
<tr>
<td></td>
<td>show lldp</td>
<td>2114</td>
</tr>
<tr>
<td></td>
<td>show lldp local-information</td>
<td>2117</td>
</tr>
<tr>
<td></td>
<td>show lldp neighbors</td>
<td>2120</td>
</tr>
<tr>
<td></td>
<td>show lldp remote-global-statistics</td>
<td>2129</td>
</tr>
<tr>
<td></td>
<td>show lldp statistics</td>
<td>2131</td>
</tr>
<tr>
<td>Chapter 23</td>
<td>MVRP Operational Commands</td>
<td>2135</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>show mvrp</td>
<td>2136</td>
</tr>
<tr>
<td></td>
<td>show mvrp applicant-state</td>
<td>2139</td>
</tr>
<tr>
<td></td>
<td>show mvrp dynamic-vlan-memberships</td>
<td>2142</td>
</tr>
<tr>
<td></td>
<td>show mvrp interface</td>
<td>2144</td>
</tr>
<tr>
<td></td>
<td>show mvrp registration-state</td>
<td>2146</td>
</tr>
<tr>
<td></td>
<td>show mvrp statistics</td>
<td>2148</td>
</tr>
<tr>
<td>Chapter 24</td>
<td>OSPF Operational Commands</td>
<td>2153</td>
</tr>
<tr>
<td></td>
<td>clear (ospf</td>
<td>ospf3) database</td>
</tr>
<tr>
<td></td>
<td>clear (ospf</td>
<td>ospf3) io-statistics</td>
</tr>
<tr>
<td></td>
<td>clear (ospf</td>
<td>ospf3) neighbor</td>
</tr>
<tr>
<td></td>
<td>clear (ospf</td>
<td>ospf3) overload</td>
</tr>
<tr>
<td></td>
<td>clear (ospf</td>
<td>ospf3) statistics</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) backup coverage</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) backup lsp</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) backup neighbor</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) backup spf</td>
</tr>
<tr>
<td></td>
<td>show ospf context-identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show ospf database</td>
<td>2180</td>
</tr>
<tr>
<td></td>
<td>show ospf3 database</td>
<td>2191</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) interface</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) io-statistics</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) log</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) neighbor</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) overview</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) route</td>
</tr>
<tr>
<td></td>
<td>show (ospf</td>
<td>ospf3) statistics</td>
</tr>
<tr>
<td>Chapter 25</td>
<td>Protocol-Independent Routing Operational Commands</td>
<td>2239</td>
</tr>
<tr>
<td></td>
<td>show as-path</td>
<td>2241</td>
</tr>
<tr>
<td></td>
<td>show as-path domain</td>
<td>2246</td>
</tr>
<tr>
<td></td>
<td>show as-path summary</td>
<td>2249</td>
</tr>
<tr>
<td></td>
<td>show route</td>
<td>2251</td>
</tr>
<tr>
<td></td>
<td>show route active-path</td>
<td>2273</td>
</tr>
<tr>
<td></td>
<td>show route advertising-protocol</td>
<td>2278</td>
</tr>
<tr>
<td></td>
<td>show route all</td>
<td>2284</td>
</tr>
<tr>
<td></td>
<td>show route aspath-regex</td>
<td>2286</td>
</tr>
<tr>
<td></td>
<td>show route best</td>
<td>2288</td>
</tr>
<tr>
<td></td>
<td>show route brief</td>
<td>2291</td>
</tr>
<tr>
<td></td>
<td>show route ccc</td>
<td>2293</td>
</tr>
<tr>
<td></td>
<td>show route community</td>
<td>2295</td>
</tr>
<tr>
<td></td>
<td>show route community-name</td>
<td>2297</td>
</tr>
<tr>
<td></td>
<td>show route damping</td>
<td>2299</td>
</tr>
<tr>
<td></td>
<td>show route detail</td>
<td>2304</td>
</tr>
<tr>
<td></td>
<td>show route exact</td>
<td>2325</td>
</tr>
<tr>
<td></td>
<td>show route export</td>
<td>2327</td>
</tr>
<tr>
<td></td>
<td>show route export vrf-target</td>
<td>2330</td>
</tr>
<tr>
<td></td>
<td>show route extensive</td>
<td>2332</td>
</tr>
</tbody>
</table>
show route flow validation ................................................. 2351
show route forwarding-table ............................................ 2354
show route forwarding-table interface-name .......................... 2372
show route hidden ....................................................... 2375
show route inactive-path ............................................... 2378
show route inactive-prefix .............................................. 2382
show route instance ...................................................... 2384
show route label ......................................................... 2392
show route label-switched-path ........................................ 2397
show route localization .................................................. 2399
show route martians ...................................................... 2401
show route match-prefix ................................................ 2404
show route next-hop ....................................................... 2405
show route no-community .............................................. 2411
show route output ....................................................... 2414
show route protocol .................................................... 2419
show route range ......................................................... 2433
show route receive-protocol ............................................ 2438
show route resolution .................................................... 2448
show route snooping ....................................................... 2453
show route source-gateway .............................................. 2456
show route summary ..................................................... 2462
show route table ........................................................ 2466
show route terse ........................................................ 2509

**Chapter 26**

**RIP Operational Commands** ........................................... 2513

  clear rip general-statistics ........................................ 2514
  clear rip statistics .................................................. 2515
  show rip general-statistics ......................................... 2517
  show rip neighbor .................................................... 2519
  show rip statistics .................................................. 2522

**Chapter 27**

**RIPng Operational Commands** ....................................... 2525

  clear ripng general-statistics ...................................... 2526
  clear ripng statistics ............................................... 2527
  show ripng general-statistics ...................................... 2528
  show ripng neighbor ................................................ 2530
  show ripng statistics ............................................... 2532

**Chapter 28**

**Firewall Filter Operational Commands** ............................. 2535

  clear firewall ....................................................... 2536
  show firewall ....................................................... 2538
  show firewall filter version ....................................... 2546
  show firewall log .................................................... 2547
  show firewall prefix-action-stats .................................. 2550
  show firewall templates-in-use .................................... 2552
  show policer ........................................................ 2554
Chapter 29  Layer 2 Bridging and Switching Operational Commands .............. 2557

- clear bridge mac-table .................................................. 2558
- clear error bpdu interface ............................................ 2559
- clear error mac-rewrite ............................................... 2560
- show bridge domain ..................................................... 2561
- show bridge flood ....................................................... 2563
- show bridge mac-table ................................................ 2570
- show bridge statistics ............................................... 2576
- show l2-learning global-information .............................. 2579
- show l2-learning global-mac-count ............................... 2581
- show l2-learning instance .......................................... 2582
- show l2-learning interface ......................................... 2584
- show mac-rewrite interface ..................................... 2586

Chapter 30  VPN Operational Commands ............................................. 2589

- clear vpls mac-address .............................................. 2590
- clear vpls mac-table .................................................. 2591
- request l2circuit-switchover ..................................... 2592
- show dynamic-tunnels database .................................. 2593
- show hfrr profiles ....................................................... 2597
- show ingress-replication mvpn .................................... 2599
- show l2circuit connections ....................................... 2601
- show l2vpn connections ............................................. 2609
- show mvpn c-multicast ............................................... 2616
- show mvpn instance .................................................. 2619
- show mvpn neighbor .................................................. 2623
- show vpls connections .............................................. 2628
- show vpls flood event-queue ..................................... 2639
- show vpls flood instance .......................................... 2641
- show vpls flood route ............................................... 2643
- show vpls mac-table .................................................. 2645
- show vpls statistics .................................................. 2651
# List of Figures

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Router Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Router Interfaces Overview</td>
</tr>
<tr>
<td>Figure 1: APS Interface</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2: Container Interface</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3: Routing Matrix</td>
<td>24</td>
</tr>
<tr>
<td>Figure 4: Routing Matrix Based on a TX Matrix Plus Router</td>
<td>26</td>
</tr>
<tr>
<td>Figure 5: Interface Slot, PIC, and Port Locations</td>
<td>29</td>
</tr>
</tbody>
</table>

| Chapter 2 | Configuring Physical Interface Properties | 47 |
| Figure 6: Two Router Interfaces Connected Through Transport Equipment | 143 |
| Figure 7: Multiple Flaps of Short Duration (Milliseconds) | 144 |
| Figure 8: Periodic Flaps of Long Duration (Seconds) | 145 |
| Figure 9: Physical-Level Link Is Down When the Penalty Falls Below the Reuse Level | 147 |
| Figure 10: Physical-Level Link Is Up When the Penalty Falls Below the Reuse Level | 148 |

| Chapter 4 | Configuring Protocol Family and Interface Address Properties | 187 |
| Figure 11: Hierarchical Policer | 215 |
| Figure 12: Unicast RPF with Routing Asymmetry | 229 |
| Figure 13: Prefix Accounting with Source and Destination Classes | 242 |
| Figure 14: Prefix Accounting with Source and Destination Classes | 245 |

| Chapter 5 | Configuring Circuit and Translational Cross-Connects | 255 |
| Figure 15: Layer 2 Switching Circuit Cross-Connect | 256 |
| Figure 16: Example Topology of a Switching Circuit Cross-Connect with Frame Relay CCC Encapsulation | 268 |
| Figure 17: Layer 2.5 Switching Translational Cross-Connect | 269 |
| Figure 18: Interface-to-Interface Circuit Cross-Connect over Aggregated Ethernet Interfaces | 271 |
| Figure 19: Remote Interface-LSP-Interface Circuit Cross-Connect over Aggregated Ethernet Interfaces | 272 |
| Figure 20: ATM-to-Ethernet Interworking | 274 |

<table>
<thead>
<tr>
<th>Part 3</th>
<th>Serial Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 10</td>
<td>Configuring Serial Interfaces</td>
</tr>
<tr>
<td>Figure 21: Serial Interface Clocking Mode</td>
<td>322</td>
</tr>
<tr>
<td>Figure 22: Serial Interface LIU Loopback</td>
<td>328</td>
</tr>
<tr>
<td>Figure 23: Serial Interface Local Loopback</td>
<td>329</td>
</tr>
</tbody>
</table>
List of Tables

About the Documentation ................................................. xli
Table 1: Notice Icons ........................................................... xliii
Table 2: Text and Syntax Conventions ..................................... xlv

Part 1 Router Interfaces
Chapter 1 Router Interfaces Overview .................................... 3
Table 3: FPC Numbering for T640 Routers in a Routing Matrix .......... 25
Table 4: One-to-One FPC Numbering for T640 Routers in a Routing Matrix ... 25
Table 5: FPC Numbering for T1600 Routers in a Routing Matrix .......... 27
Table 6: One-to-One FPC Numbering for T1600 Routers in a Routing Matrix ... 27
Table 7: Encapsulation Support by Interface Type ....................... 31

Chapter 2 Configuring Physical Interface Properties ................. 47
Table 8: Statements for Physical Interface Properties ................. 58
Table 9: Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers .......... 86
Table 10: Media MTU Sizes by Interface Type for M40e Routers ......... 87
Table 11: Media MTU Sizes by Interface Type for M160 Routers ........ 88
Table 12: Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers .......... 89
Table 13: Media MTU Sizes by Interface Type for MX Series Routers .... 90
Table 14: Media MTU Sizes by Interface Type for T320 Routers ........ 91
Table 15: Media MTU Sizes by Interface Type for T640 Platforms .......... 92
Table 16: Media MTU Sizes by Interface Type for EX Series Switches and ACX
Series Routers ........................................................... 92
Table 17: Media MTU Sizes by Interface Type for PTX Series Packet Transport
Routers .............................................................. 93
Table 18: Encapsulation Overhead by Encapsulation Type .......... 95
Table 19: Media MTU Sizes by Interface Type for ACX Series Routers .... 96
Table 20: Encapsulation Overhead by Encapsulation Type .......... 97
Table 21: Effect of set interfaces disable <interface_name> on T series PICs ... 160

Chapter 3 Configuring Logical Interface Properties ................... 161
Table 22: Statements for Logical Interface Properties ................. 165

Chapter 4 Configuring Protocol Family and Interface Address Properties .... 187
Table 23: Protocol Family Configuration Tasks .......................... 190

Part 3 Serial Interfaces
Chapter 10 Configuring Serial Interfaces ............................... 317
Table 58: show ancp summary Output Fields ............................................ 1706
Table 59: show ancp summary neighbor Output Fields ............................... 1708
Table 60: show ancp summary subscriber Output Fields ......................... 1710

Chapter 16  BFD Operational Commands ............................................. 1713
Table 61: show bfd session Output Fields ............................................. 1719

Chapter 17  BGP Operational Commands ............................................. 1729
Table 62: show bgp bmp Output Fields ................................................. 1736
Table 63: show bgp group Output Fields .............................................. 1738
Table 64: show bgp group traffic-statistics Output Fields ....................... 1745
Table 65: show bgp neighbor Output Fields .......................................... 1749
Table 66: show bgp replication Output Fields ....................................... 1769
Table 67: show bgp summary Output Fields ......................................... 1772
Table 68: show policy damping Output Fields ...................................... 1778

Chapter 18  ES-IS Operational Commands ............................................. 1779
Table 69: show esis adjacency Output Fields ....................................... 1782
Table 70: show esis interface Output Fields ....................................... 1785
Table 71: show esis statistics Output Fields ....................................... 1787

Chapter 19  IP Multicast Operational Commands ................................... 1789
Table 72: show amt statistics Output Fields ....................................... 1830
Table 73: show amt summary Output Fields ....................................... 1833
Table 74: show amt tunnel Output Fields .......................................... 1836
Table 75: show dvmrp interfaces Output Fields ................................... 1839
Table 76: show dvmrp neighbors Output Fields ................................... 1842
Table 77: show dvmrp prefix Output Fields ....................................... 1844
Table 78: show dvmrp prunes Output Fields ....................................... 1847
Table 79: show igmp group Output Fields .......................................... 1850
Table 80: show igmp interface Output Fields ..................................... 1854
Table 81: show igmp snooping interface Output Fields ......................... 1858
Table 82: show igmp snooping membership Output Fields ...................... 1864
Table 83: show igmp snooping statistics Output Fields .......................... 1870
Table 84: show igmp statistics Output Fields ..................................... 1875
Table 85: show mld group Output Fields ........................................... 1877
Table 86: show mld interface Output Fields ....................................... 1881
Table 87: show mld statistics Output Fields ....................................... 1885
Table 88: show msdp Output Fields .................................................. 1888
Table 89: show msdp source Output Fields ....................................... 1892
Table 90: show msdp source-active Output Fields ................................ 1894
Table 91: show msdp statistics Output Fields .................................... 1896
Table 92: show multicast backup-pe-groups Output Fields ..................... 1900
Table 93: show multicast flow-map Output Fields ................................ 1902
Table 94: show multicast forwarding-cache statistics Output Fields ......... 1904
Table 95: show multicast interface Output Fields ................................ 1906
Table 96: show multicast mrinfo Output Fields .................................. 1909
Table 97: show multicast next-hops Output Fields ............................... 1912
Table 98: show multicast pim-to-igmp-proxy Output Fields ..................... 1916
Table 99: show multicast pim-to-mld-proxy Output Fields ...................... 1917
Chapter 20 IPv6 Operational Commands .................................... 2035
Table 123: show ipv6 neighbors Output Fields .......................... 2040
Table 124: show ipv6 router-advertisement Output Fields .......... 2043

Chapter 21 IS-IS Operational Commands ................................. 2045
Table 125: show isis adjacency Output Fields ......................... 2055
Table 126: show isis authentication Output Fields .................. 2060
Table 127: show isis backup coverage Output Fields ................ 2061
Table 128: show isis backup label-switched-path Output Fields .... 2063
Table 129: show isis backup spf results Output Fields ............... 2066
Table 130: show isis context-identifier Output Fields ............... 2069
Table 131: show isis database Output Fields .......................... 2072
Table 132: show isis hostname Output Fields .......................... 2085
Table 133: show isis interface Output Fields .......................... 2088
Table 134: show isis overview Output Fields ......................... 2092
Table 135: show isis route Output Fields .............................. 2098
Table 136: show isis spf Output Fields ................................. 2103
Table 137: show isis statistics Output Fields ......................... 2108

Chapter 22 LLDP Operational Commands ................................. 2111
Table 138: show lldp Output Fields ..................................... 2114
Table 139: show lldp local-information Output Fields .............. 2117
Table 140: show lldp neighbors Output Fields ....................... 2121
Table 141: show lldp neighbors detail Output Fields ................. 2122
Table 142: show lldp remote-global-statistics Output Fields ....... 2129
Table 143: show lldp statistics Output Fields ........................ 2131
Chapter 23  MVRP Operational Commands ...................................2135
Table 144: show mvrp Output Fields ....................................2136
Table 145: show mvrp applicant-state Output Fields ..............2139
Table 146: show mvrp dynamic-vlan-memberships Output Fields .2142
Table 147: show mvrp interface Output Fields ......................2144
Table 148: show mvrp registration-state Output Fields ..........2146
Table 149: show mvrp statistics Output Fields .....................2149
Table 150: show mvrp statistics Output Fields .....................2150

Chapter 24  OSPF Operational Commands ................................2153
Table 151: show (ospf | ospf3) backup coverage Output Fields ....2165
Table 152: show (ospf | ospf3) backup lsp Output Fields ........2167
Table 153: show (ospf | ospf3) backup neighbor Output Fields ...2170
Table 154: show (ospf | ospf3) backup spf Output Fields ........2172
Table 155: show ospf context-identifier Output Fields ...........2179
Table 156: show ospf database Output Fields ......................2181
Table 157: show ospf3 database Output Fields .....................2193
Table 158: show (ospf | ospf3) interface Output Fields ..........2203
Table 159: show (ospf | ospf3) io-statistics Output Fields ........2208
Table 160: show (ospf | ospf3) log Output Fields .................2211
Table 161: show (ospf | ospf3) neighbor Output Fields ..........2214
Table 162: show ospf overview Output Fields ......................2221
Table 163: show (ospf | ospf3) route Output Fields ...............2227
Table 164: show (ospf | ospf3) statistics Output Fields ..........2234

Chapter 25  Protocol-Independent Routing Operational Commands ....2239
Table 165: show as-path Output Fields .........................2242
Table 166: show as-path domain Output Fields ..................2246
Table 167: show as-path summary Output Fields ..................2249
Table 168: show route Output Fields ..........................2252
Table 169: show route advertising-protocol Output Fields ....2279
Table 170: show route damping Output Fields .................2300
Table 171: show route detail Output Fields .....................2304
Table 172: Next-hop Types Output Field Values ..................2310
Table 173: State Output Field Values ..........................2312
Table 174: Communities Output Field Values ....................2314
Table 175: show route export Output Fields ....................2328
Table 176: show route export vrf-target Output Fields .......2330
Table 177: show route extensive Output Fields ..................2332
Table 178: show route flow validation Output Fields ..........2352
Table 179: show route forwarding-table Output Fields .........2357
Table 180: show route forwarding-table interface-name Output Fields 2372
Table 181: show route instance Output Fields ....................2385
Table 182: show route localization Output Fields ...............2399
Table 183: show route martians Output Fields ...................2401
Table 184: show route receive-protocol Output Fields ........2439
Table 185: show route resolution Output Fields .................2450
Table 186: show route summary Output Fields ....................2463
Table 187: show route table Output Fields ......................2467
Table 188: Next-hop Types Output Field Values ........................................ 2473
Table 189: State Output Field Values ...................................................... 2475
Table 190: Communities Output Field Values ......................................... 2477
Table 191: show route terse Output Fields ............................................. 2509

Chapter 26  RIP Operational Commands .............................................. 2513
Table 192: show rip general-statistics Output Fields ................................. 2517
Table 193: show rip neighbor Output Fields ........................................... 2520
Table 194: show rip statistics Output Fields ........................................... 2523

Chapter 27  RIPng Operational Commands ........................................... 2525
Table 195: show ripng general-statistics Output Fields ......................... 2528
Table 196: show ripng neighbor Output Fields .................................... 2530
Table 197: show ripng statistics Output Fields .................................... 2533

Chapter 28  Firewall Filter Operational Commands ............................... 2535
Table 198: show firewall Output Fields ................................................ 2540
Table 199: show firewall filter version Output Fields .......................... 2546
Table 200: show firewall log Output Fields ........................................ 2547
Table 201: show firewall prefix-action-stats Output Fields .................. 2551
Table 202: show firewall templates-in-use Output Fields ..................... 2552
Table 203: show policer Output Fields .............................................. 2555

Chapter 29  Layer 2 Bridging and Switching Operational Commands .......... 2557
Table 204: show bridge mac-table Output Fields ................................. 2571
Table 205: show l2-learning global-information Output Fields .......... 2579
Table 206: show l2-learning instance Output Fields ........................... 2582
Table 207: show l2-learning interface Output Fields ............................ 2584
Table 208: show mac-rewrite interface Output Fields .......................... 2586

Chapter 30  VPN Operational Commands ............................................. 2589
Table 209: show dynamic-tunnels database Output Fields ................. 2593
Table 210: show hfrr profiles Output Fields ................................... 2597
Table 211: show ingress-replication mvpn Output Fields ................... 2599
Table 212: show l2circuit connections Output Fields ....................... 2602
Table 213: show l2vpn connections Output Fields .............................. 2610
Table 214: show mvpn c-multicast Output Fields ............................... 2616
Table 215: show mvpn instance Output Fields ................................... 2619
Table 216: show mvpn neighbor Output Fields .................................. 2623
Table 217: show vpls connections Output Fields ................................ 2629
Table 218: show vpls flood event-queue Output Fields .................... 2639
Table 219: show vpls flood instance Output Fields ............................ 2641
Table 220: show vpls flood route Output Fields ................................ 2643
Table 221: show vpls mac-table Output fields .................................. 2646
Table 222: show vpls statistics Output Fields .................................... 2651
About the Documentation

- Documentation and Release Notes on page xli
- Using the Examples in This Manual on page xli
- Documentation Conventions on xliii
- Documentation Feedback on page xlv
- Requesting Technical Support on page xlv

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 xliii 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>!</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>!</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>!</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>!</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td>!</td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td>!</td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

Table 2 on page xlv 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:</td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Introduces or emphasizes important new terms.</td>
<td>• A policy term is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Identifies guide names.</td>
<td></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Identifies RFC and internet draft titles.</td>
<td></td>
</tr>
<tr>
<td><strong>Text like this</strong></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><strong>&lt; &gt; (angle brackets)</strong></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><strong># (pound sign)</strong></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><strong>[ ] (square brackets)</strong></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><strong>Indentation and braces ( {} )</strong></td>
<td>Identifies a level in the configuration hierarchy.</td>
<td>[edit] routing-options { static { route default { nexthop address; retain; } } }</td>
</tr>
<tr>
<td><strong>;(semicolon)</strong></td>
<td>Identifies a leaf statement at a configuration hierarchy level.</td>
<td></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/.
- 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/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: 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.
- 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/.
PART 1

Router Interfaces

- Router Interfaces Overview on page 3
- Configuring Physical Interface Properties on page 47
- Configuring Logical Interface Properties on page 161
- Configuring Protocol Family and Interface Address Properties on page 187
- Configuring Circuit and Translational Cross-Connects on page 255
CHAPTER 1

Router Interfaces Overview

- Router Interfaces Overview on page 4
- Types of Interfaces Overview on page 4
- Understanding Permanent Interfaces on page 5
- Understanding Transient Interfaces on page 5
- Understanding Services Interfaces on page 7
- Understanding Container Interfaces on page 8
- Understanding Management Ethernet Interfaces on page 10
- Understanding Interfaces on ACX Series Universal Metro Routers on page 10
- TX Matrix Plus and T1600 Router (Routing Matrix) Management Ethernet Interfaces on page 13
- Understanding Internal Ethernet Interfaces on page 14
- T1600 Routers (Routing Matrix) Internal Ethernet Interfaces on page 16
- Interface Naming Overview on page 16
- Interface Encapsulations Overview on page 31
- Interface Descriptors Overview on page 42
- Physical Part of an Interface Name on page 43
- Displaying Interface Configurations Overview on page 45
Router Interfaces Overview

Routers typically contain several different types of interfaces suited to various functions. For the interfaces on a router to function, you must configure them. Specify the interface location (that is, the slot where the Flexible PIC Concentrator [FPC], Dense Port Concentrator [DPC], or Modular Port Concentrator [MPC] is installed. You must also specify the location of the Physical Interface Card [PIC] or Modular Interface Card [MIC] , and the interface type, for example, SONET/SDH, Asynchronous Transfer Mode [ATM], or Ethernet). Finally, you must specify the encapsulation type and any interface-specific properties that may apply.

You can configure interfaces that are currently present in the router, as well as interfaces that are not currently present but that are expected to be added in the future. Junos OS detects the interface once the hardware has been installed and applies the pre-set configuration to it.

To see which interfaces are currently installed in the router, issue the `show interfaces terse` operational mode command. If an interface is listed in the output, it is physically installed in the router. If an interface is not listed in the output, it is not installed in the router.

For information about which interfaces are supported on your router, see your router’s Interface Module Reference.

You can configure Junos OS class-of-service (CoS) properties to provide a variety of classes of service for different applications, including multiple forwarding classes for managing packet transmission, congestion management, and CoS-based forwarding. For more information about configuring CoS properties, see the Class of Service Feature Guide (Routers and EX9200 Switches).

Related Documentation

• Interfaces Fundamentals for Routing Devices

Types of Interfaces Overview

Interfaces can be permanent or transient, and are used for networking or services:

• Permanent interfaces—Interfaces that are always present in the router.

• Transient interfaces—Interfaces that can be inserted into or removed from the router depending on your network configuration needs.

• Networking interfaces—Interfaces, such as Ethernet or SONET/SDH interfaces, that primarily provide traffic connectivity.

• Services interfaces—Interfaces that provide specific capabilities for manipulating traffic before it is delivered to its destination.

• Container interfaces—Interfaces that support automatic protection switching (APS) on physical SONET links using a virtual container infrastructure.
Junos OS internally generates nonconfigurable interfaces which are described in *Interfaces Command Reference* and *Services Interfaces*.

### Related Documentation

- Understanding Permanent Interfaces on page 5
- Understanding Transient Interfaces on page 5
- Understanding Services Interfaces on page 7 and *Junos OS Services Interfaces Library for Routing Devices*
- Understanding Container Interfaces on page 8
- See also the following sections regarding specific networking interface technologies used in your routers:
  - ATM Interfaces Overview
  - Channelized Interfaces Overview
  - Circuit Emulation Interfaces: *Understanding Mobile Backhaul*
  - E1 Interfaces Overview and E3 Interfaces Overview
  - Ethernet Interfaces Overview
  - Frame Relay Overview
  - SONET/SDH Interfaces Overview
  - T1 Interfaces Overview and T3 Interfaces Overview

### Understanding Permanent Interfaces

Permanent interfaces in the router consist of management Ethernet interfaces and internal Ethernet interfaces, which are described separately in the following topics:

- Understanding Management Ethernet Interfaces on page 10
- Understanding Internal Ethernet Interfaces on page 14

### Understanding Transient Interfaces

The M Series, MX Series, and T Series routers contain slots for installing Flexible PIC Concentrator [FPC] or Dense Port Concentrator [DPC] (for MX Series routers) or Modular Port Concentrator [MPC] (for MX Series routers). Physical Interface Card [PIC] can be installed in FPCs. Modular Interace Card [MIC] can be inserted into MPCs.

The number of PICs that can be installed varies by router and type of FPC. The PICs provide the actual physical interfaces to the network. The MX Series routers contain slots for installing either DPC boards that provide the physical interfaces to the network or for installing FPCs in which PICs can be installed.

You can insert any DPC or FPC into any slot that supports them in the appropriate router. Typically, you can place any combination of PICs, compatible with your router, in any location on an FPC. (You are limited by the total FPC bandwidth, and by the fact that
some PICs physically require two or four of the PIC locations on the FPC. In some cases, power limitations or microcode limitations may also apply.) To determine DPC and PIC compatibility, see the see your router’s *Interface Module Reference*.

You can insert MPC into any slot that supports them in the appropriate router. You can install up to two MICs of different media types in the same MPC as long as the MPC supports those MICs.

These physical interfaces are transient interfaces of the router. They are referred to as transient because you can hot-swap a DPC or FPC or MPC and its PICs or MICs at any time.

You must configure each transient interface based on the slot in which the FPC or DPC or MPC is installed, the location in which the PIC or MIC is installed, and for multiple port PICs or MICs, the port to which you are connecting.

You can configure the interfaces on PICs or MICs that are already installed in the router as well as interfaces on PICs or MICs that you plan to install later. The Junos OS detects which interfaces are actually present, so when the software activates its configuration, it activates only the present interfaces and retains the configuration information for the interfaces that are not present. When the Junos OS detects that an FPC containing PICs or MPC containing MICs has been inserted into the router, the software activates the configuration for those interfaces.

**Related Documentation**

- Types of Interfaces Overview on page 4
- Understanding Permanent Interfaces on page 5
- Understanding Management Ethernet Interfaces on page 10
- Understanding Internal Ethernet Interfaces on page 14
- *Supported Routing Engines by Router*
- Understanding Services Interfaces on page 7
- Understanding Container Interfaces on page 8
- Interface Encapsulations Overview on page 31
- Interface Descriptors Overview on page 42
- Interface Naming Overview on page 16
- Displaying Interface Configurations Overview on page 45
Understanding Services Interfaces

Services interfaces enable you to incrementally add services to your network. The Junos OS supports the following services PICs:

- **Adaptive Services (AS) PICs**—Allow you to provide multiple services on a single PIC by configuring a set of services and applications. The AS PICs offer a special range of services you configure in one or more service sets.

- **ES PIC**—Provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

- **Monitoring Services PICs**—Enable you to monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to gather and export detailed information about IPv4 traffic flows between source and destination nodes in your network; sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format; perform discard accounting on an incoming traffic flow; encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both; and direct filtered traffic to different packet analyzers and present the data in its original format. On a Monitoring Services PIC, you can configure either monitoring interfaces or collector interfaces. A collector interface allows you to combine multiple cflowd records into a compressed ASCII data file and export the file to an FTP server.

- **Multilink Services, MultiServices, Link Services, and Voice Services PICs**—Enable you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members.

- **Tunnel Services PIC**—By encapsulating arbitrary packets inside a transport protocol, tunneling provides a private, secure path through an otherwise public network. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and Multiprotocol Label Switching (MPLS).

- **On M Series and T Series routers, logical tunnel interfaces allow you to connect logical systems, virtual routers, or VPN instances. For more information about VPNs, see the Junos OS VPNs Library for Routing Devices. For more information about configuring tunnels, see the Junos OS Services Interfaces Library for Routing Devices.**

Related Documentation

- Types of Interfaces Overview on page 4
Understanding Container Interfaces

Container interfaces provide the following features:

- Automatic protection switching (APS) on SONET/SDH and ATM links are supported using the container infrastructure.
- Container physical interfaces and logical interfaces remain up on switchover.
- APS parameters are auto-copied from the container interface to the member links.

NOTE: Paired groups and true unidirectional APS are not currently supported.

For more information on SONET/SDH configuration, see Configuring Container Interfaces for APS on SONET Links.

Container interfaces features are described in the following sections:

- Understanding Traditional APS Concept on page 8
- Container Interfaces Concept on page 9
- APS Support for Container-Based Interfaces on page 9
- Autocopy of APS Parameters on page 9

Understanding Traditional APS Concept

Traditional APS is configured on two independent physical SONET/SDH interfaces: one configured as the working circuit and the other as the protect circuit (see Figure 1 on page 8). The circuit, named Circuit X in the figure, is the link between the two SONET interfaces.

Figure 1: APS Interface

Traditional APS uses routing protocols that run on each individual SONET/SDH interface (since circuit is an abstract construct, instead of being an actual interface). When the working link goes down, the APS infrastructure brings up the protect link and its underlying logical interfaces, and brings down the working link and its underlying logical interfaces.
causing the routing protocols to reconverge. This consumes time and leads to traffic loss even though the APS infrastructure has performed the switch quickly.

**Container Interfaces Concept**

To solve this problem, the Junos OS provides a soft interface construct called a container interface (see Figure 2 on page 9).

*Figure 2: Container Interface*

![](container-interface.png)

The container interface allows routing protocols to run on the logical interfaces associated with a virtual *container interface* instead of on the physical SONET/SDH and ATM interfaces. When APS switches the underlying physical link based on a fault condition, the container interface remains up, and the logical interface on the container interface does not flap. The routing protocols remain unaware of the APS switching.

**APS Support for Container-Based Interfaces**

With the container interface, APS is configured on the container interface itself. Individual member SONET/SDH and ATM links are either marked as primary (corresponding to the working circuit) or standby (corresponding to the protect circuit) in the configuration. No circuit or group name is specified in the container interface model; physical SONET/SDH and ATM links are put in an APS group by linking them to a single container interface. APS parameters are specified at the container interface level, and are propagated to the individual SONET/SDH and ATM links by the APS daemon.

**Autocopy of APS Parameters**

Typical applications require copying APS parameters from the working circuit to the protect circuit, since most of the parameters must be the same for both circuits. This is automatically done in the container interface. APS parameters are specified only once under the container physical interface configuration, and are internally copied over to the individual physical SONET/SDH and ATM links.

**Related Documentation**

- *Configuring Container Interfaces for APS on SONET Links*
- *Displaying APS Using a Container Interface with ATM Encapsulation*
Understanding Management Ethernet Interfaces

Management interfaces are the primary interfaces for accessing the device remotely. Typically, a management interface is not connected to the in-band network, but is connected instead to the device's internal network. Through a management interface you can access the device over the network using utilities such as ssh and telnet and configure the device from anywhere, regardless of its physical location. SNMP can use the management interface to gather statistics from the device.

A management interface lets authorized users and management systems connect to the device over the network. Some Juniper Networks devices have a dedicated management port on the front panel. For other types of platforms, you can configure a management interface on one of the network interfaces. This interface can be dedicated to management or shared with other traffic. Before users can access the management interface, you must configure it. Information required to set up the management interface includes its IP address and prefix. In many types of Junos OS devices (or recommended configurations), it is not possible to route traffic between the management interface and the other ports. Therefore, you should select an IP address in a separate (logical) network, with a separate prefix (netmask).

For Junos OS Evolved, use re0:mgmt-* for Routing Engine 0 and re1:mgmt-* for Routing Engine 1 management interfaces.

Understanding Interfaces on ACX Series Universal Metro Routers

The ACX Series routers support time-division multiplexing (TDM) T1 and E1 interfaces and Ethernet (1 GbE copper, 1GbE, 10 GbE, and 40 GbE fiber) interfaces to support both the legacy and evolution needs of the mobile network. Support for Power over Ethernet (PoE+) at 65 watts per port mitigates the need for additional electrical cabling for microwaves or other access interfaces.

The ACX Series routers support the following:

- **TDM T1 and E1 ports:**
  - The ACX1000 router contains eight T1 or E1 ports.
  - The ACX2000 router contains 16 T1 or E1 ports.
  - Inverse Multiplexing for ATM (IMA)

  **NOTE:** ACX5048 and ACX5096 routers do not support T1 or E1 ports and Inverse Multiplexing for ATM (IMA).

- **Gigabit Ethernet ports:**
  - The ACX1000 router contains eight Gigabit Ethernet ports. The ACX1000 router also supports either four RJ45 (Cu) ports or installation of four Gigabit Ethernet small form-factor pluggable (SFP) transceivers.
The ACX2000 router contains 16 Gigabit Ethernet ports and two PoE ports. The ACX2000 router also supports installation of two Gigabit Ethernet SFP transceivers and two 10-Gigabit Ethernet SFP+ transceivers.

The ACX5448 router is a 10-Gigabit Ethernet enhanced small form-factor pluggable (SFP+) top-of-rack router with 48 SFP+ ports, and four 100-Gigabit Ethernet QSFP28 ports. Each SFP+ port can operate as a native 10-Gigabit Ethernet port, or as a 1-Gigabit Ethernet port when 1-Gigabit optics are inserted. The 48 ports on ACX5448 router can be configured as 1GE or 10GE modes and these ports are represented by \( \text{xe} \) interface type. The PIC 1 of FPC 0 has 4x100GE ports, where each port can be channelized as 1x100GE, or 1x40GE, or 4x25GE modes and these ports are represented by \( \text{et} \) interface type. By default, the port speed in PIC 1 is 100GE.

**NOTE:** The ACX5448 router do not support Pseudowire Services interface.

**NOTE:** 40GbE is supported only on ACX5048, ACX5096, and ACX5448 routers. ACX5448 router support 40GbE channeling to 10GbE.

**T1 and E1 Time-Division Multiplexing (TDM) Interfaces**

On the ACX Series routers, existing Junos OS TDM features are supported without changes to statements or functionality. The following key TDM features for T1 (\( \text{ct1} \)) interfaces and E1 (\( \text{ce1} \)) interfaces are supported:

- T1 and E1 channelization
- T1 and E1 encapsulation
- Alarms, defects, and statistics
- External and internal loopback
- TDM class of service (CoS)

T1 and E1 mode selection is at the PIC level. To set the T1 or E1 mode at the PIC level, include the `framing` statement with the `t1` or `e1` option at the `[chassis fpc slot-number pic slot-number]` hierarchy level. All ports can be T1 or E1. Mixing T1s and E1s is not supported.

**T1 or E1 BITS Interface (ACX2000)**

The ACX2000 router has a T1 or E1 building-integrated timing supply (BITS) interface that you can connect to an external clock. After you connect the interface to the external clock, you can configure the BITS interface so that the BITS interface becomes a candidate source for chassis synchronization to the external clock. The frequency of the BITS interface depends on the Synchronous Ethernet equipment slave clock (EEC) selected with the `network-option` statement at the `[edit chassis synchronization]` hierarchy level.
NOTE: The ACX1000 router does not support the BITS interface.

Inverse Multiplexing for ATM (IMA)

Defined by the ATM Forum, IMA specification version 1.1 is a standardized technology used to transport ATM traffic over a bundle of T1 and E1 interfaces, also known as an IMA group. Up to eight links per bundle and 16 bundles per PIC are supported. The following key IMA features are supported:

• IMA Layer 2 encapsulation
• ATM CoS
• ATM policing and shaping
• Denied packets counter in the output for the `show interfaces at-fpc/pic/port extensive` command

Gigabit Ethernet interfaces

On the ACX Series routers, existing Junos OS Ethernet features are supported without changes to statements or functionality. The following key features are supported:

• Media type specification (ACX1000 router with Gigabit Ethernet SFP and RJ45 interfaces)
• Autonegotiation for RJ45 Gigabit Ethernet interfaces
• Event handling of SFP insertion and removal
• Explicit disabling of the physical interface
• Flow control

NOTE: The ACX Series router does not support flow control based on PAUSE frames.

• Loopback
• Loss of signal (LOS) alarm
• Media access control (MAC) layer features
• Maximum transmission unit (MTU)
• Remote fault notification for 10-Gigabit Ethernet interfaces
• Statistics collection and handling
• Power over Ethernet (PoE) (ACX2000 router)
• High power mode
The Gigabit Ethernet ports on the router have the capacity to work as a 1 or 10-Gigabit Ethernet interface, depending on the type of small form-factor pluggable (SFP) transceiver inserted. When you insert an SFP+ transceiver, the interface works at the 10-Gigabit speed. When you insert an SFP transceiver, the interface works at the 1-Gigabit speed. Configuration is not required because the speed is determined automatically based on the type of inserted SFP transceiver. The dual-speed interface is automatically created with the `xe` prefix, for example, `xe-4/0/0`.

The same configuration statements are used for both speeds and CoS parameters are scaled as a percentage of the port speed. To configure a dual-speed Gigabit Ethernet interface, include the `interface xe-fpc/pic/port` statement at the `[edit interfaces]` hierarchy level. To display the interface speed and other details, issue the `show interfaces` command.

NOTE: You need to use industrial grade of SFP below 0dC for ACX 1100 and ACX 2100 boards.

Related Documentation
- Understanding Encapsulation on an Interface
- Configuring Inverse Multiplexing for ATM (IMA) on ACX Series
- Interface Names for ACX Series Universal Metro Routers on page 43

TX Matrix Plus and T1600 Router (Routing Matrix) Management Ethernet Interfaces

For TX Matrix Plus Routers and for T1600 Core Routers with RE-C1800 configured in a routing matrix, the Junos OS automatically creates the router's management Ethernet interface, `em0`. To use `em0` as a management port, you must configure its logical port, `em0.0`, with a valid IP address.

When you enter the `show interfaces` command on a TX Matrix Plus router, the management Ethernet interfaces (and logical interfaces) are displayed:

```
user@host> show interfaces ?
... em0 em0.0 ...
```

NOTE: The Routing Engines in the TX Matrix Plus router and in the T1600 routers with RE-C1800 configured in a routing matrix do not support the management Ethernet interface `fxp0`, or the internal Ethernet interfaces `fxp1` or `fxp2`.

Related Documentation
- Understanding Internal Ethernet Interfaces on page 14
- T1600 Routers (Routing Matrix) Internal Ethernet Interfaces on page 16
Understanding Internal Ethernet Interfaces

Within a router or packet transport router, internal Ethernet interfaces provide communication between the Routing Engine and the Packet Forwarding Engines. The Junos OS automatically configures internal Ethernet interfaces when the Junos OS boots. The Junos OS boots the packet-forwarding component hardware. When these components are running, the Control Board uses the internal Ethernet interface to transmit hardware status information to the Routing Engine. Information transmitted includes the internal router temperature, the condition of the fans, whether an FPC has been removed or inserted, and information from the LCD on the craft interface.

To determine the supported internal Ethernet interfaces for your router, see Supported Routing Engines by Router.

**NOTE:** Do not modify or remove the configuration for the internal Ethernet interface that the Junos OS automatically configures. If you do, the router or packet transport router will stop functioning.

- **M Series, and MX Series routers and T Series routers**—The Junos OS creates the internal Ethernet interface. The internal Ethernet interface connects the Routing Engine re0 to the Packet Forwarding Engines.

  If the router has redundant Routing Engines, another internal Ethernet interface is created on each Routing Engine (re0 and re1) in order to support fault tolerance, two physical links between re0 and re1 connect the independent control planes. If one of the links fails, both Routing Engines can use the other link for IP communication.

- **TX Matrix Plus routers**—On a TX Matrix Plus router, the Routing Engine and Control Board function as a unit, or host subsystem. For each host subsystem in the router, the Junos OS automatically creates two internal Ethernet interfaces, ixgbe0 and ixgbe1. The ixgbe0 and ixgbe1 interfaces connect the TX Matrix Plus Routing Engine to the Routing Engines of every line-card chassis (LCC) configured in the routing matrix.

  The TX Matrix Plus Routing Engine connects to a high-speed switch through a 10-Gbps link within the host subsystem. The switch provides a 1-Gbps link to each T1600 Routing Engine. The 1-Gbps links are provided through the UTP Category 5 Ethernet cable connections between the TXP-CBs and the LCC-CBs in the LCCs.

  - The TX Matrix Plus Routing Engine connects to a high-speed switch in the local Control Board through a 10-Gbps link within the host subsystem.

  - The Gigabit Ethernet switch connects the Control Board to the remote Routing Engines of every LCC configured in the routing matrix.
If a TX Matrix Plus router contains redundant host subsystems, the independent control planes are connected by two physical links between the two 10-Gigabit Ethernet ports on their respective Routing Engines.

- The primary link to the remote Routing Engine is at the ixgbe0 interface; the 10-Gigabit Ethernet switch on the local Control Board also connects the Routing Engine to the 10-Gigabit Ethernet port accessed by the ixgbe1 interface on the remote Routing Engine.

- The alternate link to the remote Routing Engine is the 10-Gigabit Ethernet port at the ixgbe1 interface. This second port connects the Routing Engine to the 10-Gigabit Ethernet switch on the remote Control Board, which connects to the 10-Gigabit Ethernet port at the ixgbe0 interface on the remote Routing Engine.

If one of the two links between the host subsystems fails, both Routing Engines can use the other link for IP communication.

- LCC in a routing matrix—On an LCC configured in a routing matrix, the Routing Engine and Control Board function as a unit, or host subsystem. For each host subsystem in the LCC, the Junos OS automatically creates two internal Ethernet interfaces, bcm0 and em1, for the two Gigabit Ethernet ports on the Routing Engine.

  The bcm0 interface connects the Routing Engine in each LCC to the Routing Engines of every other LCC configured in the routing matrix.

  - The Routing Engine connects to a Gigabit Ethernet switch on the local Control Board through a.
  
  - The switch connects the Control Board to the remote Routing Engines of every other LCC configured in the routing matrix.

If an LCC in a routing matrix contains redundant host subsystems, the independent control planes are connected by two physical links between the Gigabit Ethernet ports on their respective Routing Engines.

- The primary link to the remote Routing Engine is at the bcm0 interface; the Gigabit Ethernet switch on the local Control Board also connects the Routing Engine to the Gigabit Ethernet port accessed by the em1 interface on the remote Routing Engine.

- The alternate link to the remote Routing Engine is at the em1 interface. This second port connects the Routing Engine to the Gigabit Ethernet switch on the remote Control Board, which connects to the Gigabit Ethernet port at the bcm0 interface on the remote Routing Engine.

If one of the two links between the host subsystems fails, both Routing Engines can use the other link for IP communication.

Each router also has two serial ports, labeled console and auxiliary, for connecting tty type terminals to the router using standard PC-type tty cables. Although these ports are not network interfaces, they do provide access to the router.

Related Documentation

- Understanding Permanent Interfaces on page 5
- Supported Routing Engines by Router
On a T1600 router configured in a routing matrix, the Routing Engine (RE-TXP-LCC) and Control Board (LCC-CB) function as a unit, or host subsystem. For each host subsystem in the router, the Junos OS automatically creates two internal Ethernet interfaces, bcm0 and em1, for the two Gigabit Ethernet ports on the Routing Engine.

Interface Naming Overview

Each interface has an interface name, which specifies the media type, the slot in which the FPC or DPC is located, the location on the FPC where the PIC is installed, and the PIC or DPC port. The interface name uniquely identifies an individual network connector in the system. You use the interface name when configuring interfaces and when enabling various functions and properties, such as routing protocols, on individual interfaces. The system uses the interface name when displaying information about the interface, for example, in the `show interfaces` command.

The interface name is represented by a physical part, a channel part, and a logical part in the following format:

```
physical<:channel>.logical
```

The channel part of the name is optional for all interfaces except channelized DS3, E1, OC12, and STM1 interfaces.

The EX Series, QFX Series, NFX Series, OCX1100, QFabric System, and EX4600 devices use a naming convention for defining the interfaces that are similar to that of other platforms running under Juniper Networks Junos OS. For more information, see `Understanding Interface Naming Conventions`.

Related Documentation

- Understanding Internal Ethernet Interfaces on page 14
- Displaying Internal Ethernet Interfaces for a Routing Matrix with a TX Matrix Plus Router
- show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet) on page 1476
The following sections provide interface naming configuration guidelines:

- Physical Part of an Interface Name on page 17
- Logical Part of an Interface Name on page 23
- Separators in an Interface Name on page 23
- Channel Part of an Interface Name on page 23
- Interface Naming for a Routing Matrix Based on a TX Matrix Router on page 24
- Interface Naming for a Routing Matrix Based on a TX Matrix Plus Router on page 26
- Chassis Interface Naming on page 28
- Examples: Interface Naming on page 29

**Physical Part of an Interface Name**

The physical part of an interface name identifies the physical device, which corresponds to a single physical network connector.

---

**NOTE:**

The internal interface is dependent on the Routing Engine. To identify if the Routing Engine is using this type of interface, use the following command:

```
user@host> show interfaces terse
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>pfe-1/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfe-1/0/0.16383</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfh-1/0/0</td>
<td>up</td>
<td>up</td>
<td>inet6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfh-1/0/0.16383</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[............]</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bcm0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bcm0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1/8</td>
<td></td>
</tr>
<tr>
<td>[............]</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lsi</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mtun</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pimd</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pime</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tap</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information on the Routing Engines that each chassis supports, the first supported release for the Routing Engine in the specified chassis, the management Ethernet interface, and the internal Ethernet interfaces for each Routing Engine, please refer the link titled **Supported Routing Engines by Chassis** under Related Documentation section.

---

This part of the interface name has the following format:

```
type-fpc/pic/port
```
type is the media type, which identifies the network device that can be one of the following:

- **ae**—Aggregated Ethernet interface. This is a virtual aggregated link and has a different naming format from most PICs; for more information, see *Aggregated Ethernet Interfaces Overview*.

- **as**—Aggregated SONET/SDH interface. This is a virtual aggregated link and has a different naming format from most PICs; for more information, see *Configuring Aggregated SONET/SDH Interfaces*.

- **at**—ATMI or ATM2 intelligent queuing (IQ) interface or a virtual ATM interface on a circuit emulation (CE) interface.

- **bcm**—The bcm0 internal Ethernet process is supported on specific Routing engines for various M series and T series routers. For more information please refer the link titled *Supported Routing Engines by Chassis* under Related Documentation section.

- **cau4**—Channelized AU-4 IQ interface (configured on the Channelized STMI IQ or IQE PIC or Channelized OC12 IQ and IQE PICs).

- **cel**—Channelized E1 IQ interface (configured on the Channelized E1 IQ PIC or Channelized STMI IQ or IQE PIC).

- **ci**—Container interface.

- **coc1**—Channelized OC1 IQ interface (configured on the Channelized OC12 IQ and IQE or Channelized OC3 IQ and IQE PICs).

- **coc3**—Channelized OC3 IQ interface (configured on the Channelized OC3 IQ and IQE PICs).

- **coc12**—Channelized OC12 IQ interface (configured on the Channelized OC12 IQ and IQE PICs).

- **coc48**—Channelized OC48 interface (configured on the Channelized OC48 and Channelized OC48 IQE PICs).

- **cp**—Collector interface (configured on the Monitoring Services II PIC).

- **cstm1**—Channelized STMI IQ interface (configured on the Channelized STMI IQ or IQE PIC).

- **cstm4**—Channelized STM4 IQ interface (configured on the Channelized OC12 IQ and IQE PICs).

- **cstm16**—Channelized STM16 IQ interface (configured on the Channelized OC48/STM16 and Channelized OC48/STM16 IQE PICs).

- **ct1**—Channelized T1 IQ interface (configured on the Channelized DS3 IQ and IQE PICs, Channelized OC3 IQ and IQE PICs, Channelized OC12 IQ and IQE PICs, or Channelized T1 IQ PIC).

- **ct3**—Channelized T3 IQ interface (configured on the Channelized DS3 IQ and IQE PICs, Channelized OC3 IQ and IQE PICs, or Channelized OC12 IQ and IQE PICs).

- **demux**—Interface that supports logical IP interfaces that use the IP source or destination address to demultiplex received packets. Only one demux interface (*demux0*) exists
per chassis. All demux logical interfaces must be associated with an underlying logical interface.

- **dfc**—Interface that supports dynamic flow capture processing on T Series or M320 routers containing one or more Monitoring Services III PICs. Dynamic flow capture enables you to capture packet flows on the basis of dynamic filtering criteria. Specifically, you can use this feature to forward passively monitored packet flows that match a particular filter list to one or more destinations using an on-demand control protocol.

- **ds**—DS0 interface (configured on the Multichannel DS3 PIC, Channelized E1 PIC, Channelized OC3 IQ and IQE PICs, Channelized OC12 IQ and IQE PICs, Channelized DS3 IQ and IQE PICs, Channelized E1 IQ PIC, Channelized ST1 IQ or IQE PIC, or Channelized T1 IQ).

- **dsc**—Discard interface.

- **e1**—E1 interface (including channelized STM1-to-E1 interfaces).

- **e3**—E3 interface (including E3 IQ interfaces).

- **em**—Management and internal Ethernet interfaces. For M Series routers, MX Series routers, T Series routers, and TX Series routers, you can use the `show chassis hardware` command to display hardware information about the router, including its Routing Engine model. To determine which management interface is supported on your router and Routing Engine combination, see “Understanding Management Ethernet Interfaces” on page 10 and Supported Routing Engines by Router.

- **es**—Encryption interface.

- **et**—100-Gigabit Ethernet interfaces (10, 40, and 100-Gigabit Ethernet interface for PTX Series Packet Transport Routers only).

- **fe**—Fast Ethernet interface.

- **fxp**—Management and internal Ethernet interfaces. For M Series routers, MX Series routers, T Series routers, and TX Series routers, you can use the `show chassis hardware` command to display hardware information about the router, including its Routing Engine model. To determine which management interface is supported on your router and Routing Engine combination, see “Understanding Management Ethernet Interfaces” on page 10 and Supported Routing Engines by Router.

- **ge**—Gigabit Ethernet interface.
NOTE:

- The XENPAK 10-Gigabit Ethernet interface PIC, which is supported only on M series routers, is configured using the ge interface naming convention instead of the xe interface naming convention. Refer the following show commands for more information:

```bash
user@host> show chassis hardware
```

<table>
<thead>
<tr>
<th>FPC 4</th>
<th>REV 02</th>
<th>710-015839</th>
<th>CZ1853</th>
<th>M120 FPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC 0</td>
<td>REV 09</td>
<td>750-009567</td>
<td>NH1857</td>
<td>1x</td>
</tr>
<tr>
<td>10GE(LAN), XENPAK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xcvr 0</td>
<td>REV 01</td>
<td>740-012045</td>
<td>535TFZX6</td>
<td>XENPAK-SR</td>
</tr>
</tbody>
</table>

```bash
user@host> show configuration interfaces ge-4/0/0
```

```
unit 0 {
  family inet {
    address 100.0.0.1/24;
  }
}
```

- In MX and SRX series devices, the 1 and 10-Gigabit SFP or SFP+ optical interfaces are always named as xe even if a 1-Gigabit SFP is inserted. However, in EX and QFX series devices, the interface name is shown as ge or xe based on the speed of the optical device inserted.

- `gr`—Generic routing encapsulation (GRE) tunnel interface.

- `gre`—Internally generated interface that is configurable only as the control channel for Generalized MPLS (GMPLS). For more information about GMPLS, see the MPLS Applications Feature Guide.

NOTE: You can configure GRE interfaces (gre-x/y/z) only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications.

- `ip`—IP-over-IP encapsulation tunnel interface.

- `ipip`—Internally generated interface that is not configurable.

- `ixgbe`—The internal Ethernet process ixgbe0 and ixgbe1 are used by the RE-DUO-C2600-16G Routing Engine, which is supported on TX Matrix Plus and PTX5000.

- `iw`—Logical interfaces associated with the endpoints of Layer 2 circuit and Layer 2 VPN connections (pseudowire stitching Layer 2 VPNs). For more information about VPNs, see the Junos OS VPNs Library for Routing Devices.

- `lc`—Internally generated interface that is not configurable.
• **lo**—Loopback interface. The Junos OS automatically configures one loopback interface (**lo0**). The logical interface **lo0.16383** is a nonconfigurable interface for router control traffic.

• **ls**—Link services interface.

• **lsi**—Internally generated interface that is not configurable.

• **ml**—Multilink interface (including Multilink Frame Relay and MLPPP).

• **mo**—Monitoring services interface (including monitoring services and monitoring services II). The logical interface **mo-fpc/pic/port.16383** is an internally generated, nonconfigurable interface for router control traffic.

• **ms**—Multiservices interface.

• **mt**—Multicast tunnel interface (internal router interface for VPNs). If your router has a Tunnel PIC, the Junos OS automatically configures one multicast tunnel interface (**mt**) for each virtual private network (VPN) you configure. Although it is not necessary to configure multicast interfaces, you can use the **multicast-only** statement to configure the unit and family so that the tunnel can transmit and receive multicast traffic only. For more information, see **multicast-only**.

• **mtun**—Internally generated interface that is not configurable.

• **oc3**—OC3 IQ interface (configured on the Channelized OC12 IQ and IQE PICs or Channelized OC3 IQ and IQE PICs).

• **pd**—Interface on the rendezvous point (RP) that de-encapsulates packets.

• **pe**—Interface on the first-hop PIM router that encapsulates packets destined for the RP router.

• **pimd**—Internally generated interface that is not configurable.

• **pime**—Internally generated interface that is not configurable.

• **rlsq**—Container interface, numbered from 0 through 127, used to tie the primary and secondary LSQ PICs together in high availability configurations. Any failure of the primary PIC results in a switch to the secondary PIC and vice versa.

• **rms**—Redundant interface for two multiservices interfaces.

• **rsp**—Redundant virtual interface for the adaptive services interface.

• **se**—Serial interface (including EIA-530, V.35, and X.21 interfaces).

• **si**—Services-inline interface, which is hosted on a Trio-based line card.

• **so**—SONET/SDH interface.

• **sp**—Adaptive services interface. The logical interface **sp-fpc/pic/port.16383** is an internally generated, nonconfigurable interface for router control traffic.

• **stm1**—STM1 interface (configured on the OC3/STM1 interfaces).

• **stm4**—STM4 interface (configured on the OC12/STM4 interfaces).

• **stm16**—STM16 interface (configured on the OC48/STM16 interfaces).
• **t1**—T1 interface (including channelized DS3-to-DS1 interfaces).
• **t3**—T3 interface (including channelized OC12-to-DS3 interfaces).
• **tap**—Internally generated interface that is not configurable.
• **umd**—USB modem interface.
• **vsp**—Voice services interface.
• **vc4**—Virtually concatenated interface.
• **vt**—Virtual loopback tunnel interface.
• **xe**—10-Gigabit Ethernet interface. Some older 10-Gigabit Ethernet interfaces use the *ge* media type (rather than *xe*) to identify the physical part of the network device.
• **xt**—Logical interface for Protected System Domains to establish a Layer 2 tunnel connection.

**fpc** identifies the number of the FPC or DPC card on which the physical interface is located. Specifically, it is the number of the slot in which the card is installed.

M40, M40e, M160, M320, M120, T320, T640, and T1600 routers each have eight FPC slots that are numbered 0 through 7, from left to right as you are facing the front of the chassis. For information about compatible FPCs and PICs, see the hardware guide for your router.

On PTX1000 routers, the FPC number is always 0.

The M20 router has four FPC slots that are numbered 0 through 3, from top to bottom as you are facing the front of the chassis. The slot number is printed adjacent to each slot.

MX Series routers support DPCs, FPCs, and Modular Interface Cards (MICs). For information about compatible DPCs, FPCs, PICs, and MICs, see the *MX Series Interface Module Reference*.

For M5, M7i, M10, and M10i routers, the FPCs are built into the chassis; you install the PICs into the chassis.

The M5 and M7i routers have space for up to four PICs. The M7i router also comes with an integrated Tunnel PIC, or an optional integrated AS PIC, or an optional integrated MS PIC.

The M10 and M10i routers have space for up to eight PICs.

A routing matrix can have up to 32 FPCs (numbered 0 through 31).

For more information about interface naming for a routing matrix, see "Interface Naming for a Routing Matrix Based on a TX Matrix Router" on page 24.

**pic** identifies the number of the PIC on which the physical interface is located. Specifically, it is the number of the PIC location on the FPC. FPCs with four PIC slots are numbered 0 through 3. FPCs with three PIC slots are numbered 0 through 2. The PIC location is printed
on the FPC carrier board. For PICs that occupy more than one PIC slot, the lower PIC slot number identifies the PIC location.

*port* identifies a specific port on a PIC or DPC. The number of ports varies depending on the PIC. The port numbers are printed on the PIC.

### Logical Part of an Interface Name

The logical unit part of the interface name corresponds to the logical unit number. The range of number available varies for different interface types. See *unit* for current range values.

In the virtual part of the name, a period (.) separates the port and logical unit numbers:

- Other platforms:
  
  
  **type-fpc/pic/port.logical**

### Separators in an Interface Name

There is a separator between each element of an interface name.

In the physical part of the name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers.

In the virtual part of the name, a period (.) separates the channel and logical unit numbers.

A colon (:) separates the physical and virtual parts of the interface name.

### Channel Part of an Interface Name

The channel identifier part of the interface name is required only on channelized interfaces. For channelized interfaces, channel 0 identifies the first channelized interface. For channelized IQ and channelized IQE interfaces, channel 1 identifies the first channelized interface. A nonconcatenated (that is, channelized) SONET/SDH OC48 interface has four OC12 channels, numbered 0 through 3.

To determine which types of channelized PICs are currently installed in the router, use the `show chassis hardware` command from the top level of the command-line interface (CLI). Channelized IQ and IQE PICs are listed in the output with “intelligent queuing IQ” or “enhanced intelligent queuing IQE” in the description. For more information, see *Channelized Interfaces Overview*.

For ISDN interfaces, you specify the B-channel in the form `bc-pim/0/port:n`. *n* is the B-channel ID and can be 1 or 2. You specify the D-channel in the form `dc-pim/0/port:0`.

**NOTE:** For ISDN, the B-channel and D-channel interfaces do not have any configurable parameters. However, when interface statistics are displayed, B-channel and D-channel interfaces have statistical values.
NOTE: In the Junos OS implementation, the term *logical interfaces* generally refers to interfaces you configure by including the unit statement at the [edit interfaces *interface-name*] hierarchy level. Logical interfaces have the `.logical` descriptor at the end of the interface name, as in `ge-0/0/0.1` or `t1-0/0/0:0.1`, where the logical unit number is 1.

Although channelized interfaces are generally thought of as logical or virtual, the Junos OS sees T3, T1, and NxDS0 interfaces within a channelized IQ or IQE PIC as physical interfaces. For example, both `t3-0/0/0` and `t3-0/0/0:1` are treated as physical interfaces by the Junos OS. In contrast, `t3-0/0/0.2` and `t3-0/0/0:1.2` are considered logical interfaces because they have the `.2` at the end of the interface names.

### Interface Naming for a Routing Matrix Based on a TX Matrix Router

A routing matrix based on a Juniper Networks TX Matrix router is a multichassis architecture composed of one TX Matrix router and from one to four interconnected T640 routers. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix router controls all the T640 routers, as shown in Figure 3 on page 24.

*Figure 3: Routing Matrix*

A TX Matrix router is also referred to as a *switch-card chassis* (SCC). The CLI uses `scc` to refer to the TX Matrix router. A T640 router in a routing matrix is also referred to as a *line-card chassis* (LCC). The CLI uses `lcc` as a prefix to refer to a specific T640 router.

LCCs are assigned numbers 0 through 3, depending on the hardware setup and connectivity to the TX Matrix router. For more information, see the *TX Matrix Router Hardware Guide*. A routing matrix can have up to four T640 routers, and each T640 router has up to eight FPCs. Therefore, the routing matrix as a whole can have up to 32 FPCs (0 through 31).
In the Junos OS CLI, an interface name has the following format:

```
type-fpc/pic/port
```

When you specify the `fpc` number for a T640 router in a routing matrix, the Junos OS determines which T640 router contains the specified FPC based on the following assignment:

- On LCC 0, FPC hardware slots 0 through 7 are configured as 0 through 7.
- On LCC 1, FPC hardware slots 0 through 7 are configured as 8 through 15.
- On LCC 2, FPC hardware slots 0 through 7 are configured as 16 through 23.
- On LCC 3, FPC hardware slots 0 through 7 are configured as 24 through 31.

For example, the `1` in `se-1/0/0` refers to FPC hardware slot 1 on the T640 router labeled `lcc0`. The `11` in `t1-11/2/0` refers to FPC hardware slot 3 on the T640 router labeled `lcc1`. The `20` in `so-20/0/1` refers to FPC hardware slot 4 on the T640 router labeled `lcc2`. The `31` in `t3-31/1/0` refers to FPC hardware slot 7 on the T640 router labeled `lcc3`.

Table 3 on page 25 summarizes the FPC numbering for a T640 router in a routing matrix.

**Table 3: FPC Numbering for T640 Routers in a Routing Matrix**

<table>
<thead>
<tr>
<th>LCC Numbers Assigned to the T640 Router</th>
<th>Configuration Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 through 7</td>
</tr>
<tr>
<td>1</td>
<td>8 through 15</td>
</tr>
<tr>
<td>2</td>
<td>16 through 23</td>
</tr>
<tr>
<td>3</td>
<td>24 through 31</td>
</tr>
</tbody>
</table>

Table 4 on page 25 lists each FPC hardware slot and the corresponding configuration numbers for LCCs 0 through 3.

**Table 4: One-to-One FPC Numbering for T640 Routers in a Routing Matrix**

<table>
<thead>
<tr>
<th>FPC Numbering</th>
<th>T640 Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LCC 0</td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
</tbody>
</table>

|               | LCC 1        |
| Hardware Slots| 0 1 2 3 4 5 6 7 |
### Table 4: One-to-One FPC Numbering for T640 Routers in a Routing Matrix (continued)

<table>
<thead>
<tr>
<th>FPC Numbering</th>
<th>T640 Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Numbers</td>
<td>8</td>
</tr>
<tr>
<td>LCC 2</td>
<td></td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>16</td>
</tr>
<tr>
<td>LCC 3</td>
<td></td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>24</td>
</tr>
</tbody>
</table>

### Interface Naming for a Routing Matrix Based on a TX Matrix Plus Router

A routing matrix based on a Juniper Networks TX Matrix Plus Router is a multichassis architecture composed of one TX Matrix Plus router and from one to four interconnected T1600 routers. From the perspective of the user interface, the routing matrix appears as a single router. The TX Matrix Plus router controls all the T1600 routers, as shown in Figure 4 on page 26.

**Figure 4: Routing Matrix Based on a TX Matrix Plus Router**

A TX Matrix Plus router is also referred to as a *switch-fabric chassis* (SFC). The CLI uses `sfc` to refer to the TX Matrix Plus router. A T1600 router in a routing matrix is also referred to as a *line-card chassis* (LCC). The CLI uses `lcc` as a prefix to refer to a specific T1600 router.
LCCs are assigned numbers, 0 through 3, depending on the hardware setup and connectivity to the TX Matrix Plus router. For more information, see the TX Matrix Plus Router Hardware Guide. A routing matrix based on a TX Matrix Plus router can have up to four T1600 routers, and each T1600 router has up to eight FPCs. Therefore, the routing matrix as a whole can have up to 32 FPCs (0 through 31).

In the Junos OS CLI, an interface name has the following format:

\[ \text{type-fpc/pic/port} \]

When you specify the fpc number for a T1600 router in a routing matrix, the Junos OS determines which T1600 router contains the specified FPC based on the following assignment:

- On LCC 0, FPC hardware slots 0 through 7 are configured as 0 through 7.
- On LCC 1, FPC hardware slots 0 through 7 are configured as 8 through 15.
- On LCC 2, FPC hardware slots 0 through 7 are configured as 16 through 23.
- On LCC 3, FPC hardware slots 0 through 7 are configured as 24 through 31.

For example, the 1 in \text{se-1/0/0} refers to FPC hardware slot 1 on the T1600 router labeled \text{lcc0}. The 11 in \text{t1-11/2/0} refers to FPC hardware slot 3 on the T1600 router labeled \text{lcc1}. The 20 in \text{so-20/0/1} refers to FPC hardware slot 4 on the T1600 router labeled \text{lcc2}. The 31 in \text{t3-31/1/0} refers to FPC hardware slot 7 on the T1600 router labeled \text{lcc3}.

Table 5 on page 27 summarizes the FPC numbering for a routing matrix based on a TX Matrix Plus router.

**Table 5: FPC Numbering for T1600 Routers in a Routing Matrix**

<table>
<thead>
<tr>
<th>LCC Numbers Assigned to the T1600 Router</th>
<th>Configuration Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 through 7</td>
</tr>
<tr>
<td>1</td>
<td>8 through 15</td>
</tr>
<tr>
<td>2</td>
<td>16 through 23</td>
</tr>
<tr>
<td>3</td>
<td>24 through 31</td>
</tr>
</tbody>
</table>

Table 6 on page 27 lists each FPC hardware slot and the corresponding configuration numbers for LCCs 0 through 3.

**Table 6: One-to-One FPC Numbering for T1600 Routers in a Routing Matrix**

<table>
<thead>
<tr>
<th>FPC Numbering</th>
<th>T1600 Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCC 0 Hardware Slots</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
</tbody>
</table>
Table 6: One-to-One FPC Numbering for T1600 Routers in a Routing Matrix (continued)

<table>
<thead>
<tr>
<th>FPC Numbering</th>
<th>T1600 Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Numbers</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>LCC 1</td>
<td>76543210</td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>8 9 10 11 12 13 14 15</td>
</tr>
<tr>
<td>LCC 2</td>
<td>76543210</td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>16 17 18 19 20 21 22 23</td>
</tr>
<tr>
<td>LCC 3</td>
<td>76543210</td>
</tr>
<tr>
<td>Hardware Slots</td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>Configuration Numbers</td>
<td>24 25 26 27 28 29 30 31</td>
</tr>
</tbody>
</table>

Chassis Interface Naming

You configure some PIC properties, such as framing, at the [edit chassis] hierarchy level. Chassis interface naming varies depending on the routing hardware.

- To configure PIC properties for a standalone router, you must specify the FPC and PIC numbers, as follows:

  ```
  [edit chassis]
  fpc slot-number {
    pic pic-number {
      ...
    }
  }
  ```

- To configure PIC properties for a T640 or T1600 router configured in a routing matrix, you must specify the LCC, FPC, and PIC numbers, as follows:

  ```
  [edit chassis]
  lcc lcc-number {
    fpc slot-number { # Use the hardware FPC slot number
      pic pic-number {
        ...
      }
    }
  }
  ```
For the FPC slot in a T640 router in a routing matrix, specify the actual hardware slot number, as labeled on the T640 router chassis. Do not use the corresponding software FPC configuration numbers shown in Table 4 on page 25.

For the FPC slot in a T1600 router in a routing matrix, specify the actual hardware slot number, as labeled on the T1600 router chassis. Do not use the corresponding software FPC configuration numbers shown in Table 5 on page 27.

For more information about the [edit chassis] hierarchy, see the Junos OS Administration Library.

Examples: Interface Naming

This section provides examples of naming interfaces. For an illustration of where slots, PICs, and ports are located, see Figure 5 on page 29.

Figure 5: Interface Slot, PIC, and Port Locations

For an FPC in slot 1 with two OC3 SONET/SDH PICs in PIC positions 0 and 1, each PIC with two ports uses the following names:

- so-1/0/0.0
- so-1/0/1.0
- so-1/1/0.0
- so-1/1/1.0

An OC48 SONET/SDH PIC in slot 1 and in concatenated mode appears as a single FPC with a single PIC, which has a single port. If this interface has a single logical unit, it has the following name:

- so-1/0/0.0
An OC48 SONET/SDH PIC in slot 1 and in channelized mode has a number for each channel. For example:

so-1/0/0:0
so-1/0/0:1

For an FPC in slot 1 with a Channelized OC12 PIC in PIC position 2, the DS3 channels have the following names:

t3-1/2/0:0
t3-1/2/0:1
t3-1/2/0:2
...
t3-1/2/0:11

For an FPC in slot 1 with four OC12 ATM PICs (the FPC is fully populated), the four PICs, each with a single port and a single logical unit, have the following names:

at-1/0/0.0
at-1/1/0.0
at-1/2/0.0
at-1/3/0.0

In a routing matrix on the T640 router labeled lcc1, for an FPC in slot 5 with four SONET OC192 PICs, the four PICs, each with a single port and a single logical unit, have the following names:

so-13/0/0.0
so-13/1/0.0
so-13/2/0.0
so-13/3/0.0

For an FPC in slot 1 with one 4-port ISDN BRI interface card, port 4 has the following name:

br-1/0/4

The first B-channel, the second B-channel, and the control channel have the following names:

bc-1/0/4:1
bc-1/0/4:2
dc-1/0/4:0

Related Documentation

- Router Interfaces Overview on page 4
- Physical Part of an Interface Name on page 43
- Understanding Interface Naming Conventions
- Supported Routing Engines by Chassis
Interface Encapsulations Overview

Table 7 on page 31 lists encapsulation support by interface type.

Table 7: Encapsulation Support by Interface Type

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae—Aggregated Ethernet interface</td>
<td>ethernet-ccc—Ethernet cross-connect</td>
<td>dix—Ethernet DIXv2 (RFC 894)</td>
</tr>
<tr>
<td></td>
<td>extended-vlan-ccc—Nonstandard TPID tagging for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-vlan-vpls—Extended VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flexible-ethernet-services—Allows per-unit Ethernet encapsulation configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ethernet-vpls—Ethernet virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td>as—Aggregated SONET/SDH interface</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td></td>
</tr>
<tr>
<td>at—ATMI interface</td>
<td>atm-ccc-cell-relay—ATM cell relay encapsulation for a cross-connect</td>
<td>atm-ccc-cell-relay—ATM cell relay for CCC</td>
</tr>
<tr>
<td></td>
<td>atm-pvc—ATM permanent virtual circuits</td>
<td>atm-ccc-vc-mux—ATM VC for CCC</td>
</tr>
<tr>
<td></td>
<td>ethernet-over-atm—Ethernet over ATM encapsulation</td>
<td>atm-cisco-nlpid—Cisco-compatible ATM NLPID encapsulation</td>
</tr>
<tr>
<td></td>
<td>atm-nlpid—ATM NLPID encapsulation</td>
<td>atm-snap—ATM LLC/SNAP encapsulation</td>
</tr>
<tr>
<td></td>
<td>atm-snap—ATM LLC/SNAP encapsulation</td>
<td>atm-tcc-snap—ATM LLC/SNAP for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>atm-tcc-vc-mux—ATM VC for a translational cross-connect</td>
<td>atm-tcc-vc-mux—ATM VC for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>atm-vc-mux—ATM VC multiplexing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ether-over-atm-lc—Ethernet over ATM (LLC/SNAP) encapsulation</td>
<td></td>
</tr>
</tbody>
</table>
Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>atm—ATM2 intelligent queuing (IQ) interface</td>
<td>atm-ccc-cell-relay—ATM cell relay encapsulation for a cross-connect</td>
<td>atm-ccc-cell-relay—ATM cell relay for CCC</td>
</tr>
<tr>
<td></td>
<td>atm-pvc—ATM permanent virtual circuits</td>
<td>atm-ccc-vc-mux—ATM VC for CCC</td>
</tr>
<tr>
<td></td>
<td>ethernet-over-atm—Ethernet over ATM encapsulation</td>
<td>atm-cisco-nlpid—Cisco-compatible ATM NLPIID encapsulation</td>
</tr>
<tr>
<td></td>
<td>ether-over-atm-llc—Ethernet over ATM (LLC/SNAP) encapsulation</td>
<td>atm-milppp-llc—ATM MLPPP over AAL5/LLC</td>
</tr>
<tr>
<td></td>
<td>ether-vpls-over-atm-llc—Ethernet VPLS over ATM (bridging) encapsulation</td>
<td>atm-nlpid—ATM NLPIID encapsulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-ppp-llc—ATM PPP over AAL5/LLC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-ppp-vc-mux—ATM PPP over raw AAL5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-snap—ATM LLC/SNAP encapsulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-tcc-snap—ATM LLC/SNAP for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-tcc-vc-mux—ATM VC for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>atm-vc-mux—ATM VC multiplexing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ether-over-atm-llc—Ethernet over ATM (LLC/SNAP) encapsulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ether-vpls-over-atm-llc—Ethernet VPLS over ATM (bridging) encapsulation</td>
</tr>
<tr>
<td>bcm—Gigabit Ethernet internal interfaces</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>br—Integrated Services Digital Network (ISDN) interface</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>ci—Container interface</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>aps—SONET interface required for APS configuration.</td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ds</strong>—DS0 interface</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ppp—PPP over Frame Relay</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-tcc—Frame Relay DLCI for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td><strong>dsc</strong>—Discard interface</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Physical Interface Encapsulation</td>
<td>Logical Interface Encapsulation</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>e1—E1 interface (including channelized STMI-to-E1 interfaces)</strong></td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ppp—PPP over Frame Relay</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-tcc—Frame Relay DLCI for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td></td>
</tr>
</tbody>
</table>
Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>e3—E3 interface (including E3 IQ and IQE interfaces)</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ppp—PPP over Frame Relay</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-tcc—Frame Relay DLCI for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td>em—Management and internal Ethernet interfaces</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe—Fast Ethernet interface</td>
<td>ethernet-ccc—Ethernet cross-connect</td>
<td>dix—Ethernet DIXv2 (RFC 894)</td>
</tr>
<tr>
<td></td>
<td>ethernet-tcc—Ethernet translational cross-connect</td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
</tr>
<tr>
<td></td>
<td>ethernet-vpls—Ethernet virtual private LAN service</td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
</tr>
<tr>
<td></td>
<td>extended-vlan-ccc—Nonstandard TPID tagging for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-vlan-tcc—802.1Q tagging for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-vlan-vpls—Extended VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td>fxp—Management and internal Ethernet interfaces</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>ge—Gigabit Ethernet interface (including Gigabit Ethernet IQ interfaces)</td>
<td>ethernet-ccc—Ethernet cross-connect</td>
<td>dix—Ethernet DIXv2 (RFC 894)</td>
</tr>
<tr>
<td></td>
<td>ethernet-tcc—Ethernet translational cross-connect</td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
</tr>
<tr>
<td></td>
<td>ethernet-vpls—Ethernet virtual private LAN service</td>
<td>vlan-tcc—802.1Q tagging for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>extended-vlan-ccc—Nonstandard TPID tagging for a cross-connect</td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
</tr>
<tr>
<td></td>
<td>extended-vlan-tcc—802.1Q tagging for a translational cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extended-vlan-vpls—Extended VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flexible-ethernet-services—Allows per-unit Ethernet encapsulation configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
<td></td>
</tr>
<tr>
<td>ixgbe—10-Gigabit Ethernet internal interfaces</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>lo—Loopback interface; the Junos OS automatically configures one loopback interface (lo0)</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Physical Interface Encapsulation</td>
<td>Logical Interface Encapsulation</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>ls</strong>—Link services interface</td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
<td>multilink-frame-relay-end-to-end—Multilink Frame Relay end-to-end (FRF.15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multilink-ppp—Multilink PPP</td>
</tr>
<tr>
<td><strong>lsq</strong>—Link services IQ interface</td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
<td>multilink-frame-relay-end-to-end—Multilink Frame Relay end-to-end (FRF.15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multilink-ppp—Multilink PPP</td>
</tr>
<tr>
<td><strong>lt</strong>—Logical tunnel interface</td>
<td>NA</td>
<td>ethernet—Ethernet service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ethernet-vpls—Ethernet virtual private LAN service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ethernet-ccc—Ethernet cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan—VLAN service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan-ccc—802.1Q tagging for a cross-connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan-vpls—VLAN virtual private LAN service</td>
</tr>
<tr>
<td><strong>ml</strong>—Multilink interface (including Multilink Frame Relay and MLPPP)</td>
<td>NA</td>
<td>multilink-frame-relay-end-to-end—Multilink Frame Relay end-to-end (FRF.15)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multilink-ppp—Multilink PPP</td>
</tr>
</tbody>
</table>
### Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>se—Serial interface (including EIA-530, V.35, and X.21 interfaces)</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
</tbody>
</table>
### Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>so—SONET/SDH interface</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
</tbody>
</table>
Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1—T1 interface (including channelized DS3-to-DS1 interfaces)</td>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td></td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
</tr>
<tr>
<td></td>
<td>frame-relay—Frame Relay encapsulation</td>
<td>frame-relay—Frame Relay encapsulation</td>
</tr>
<tr>
<td></td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
</tr>
<tr>
<td></td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
</tr>
<tr>
<td></td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
</tr>
<tr>
<td></td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
<td>multilink-frame-relay-uni-nni—Multilink Frame Relay UNI NNI (FRF.16) encapsulation</td>
</tr>
<tr>
<td></td>
<td>ppp—Serial PPP device</td>
<td>ppp—Serial PPP device</td>
</tr>
<tr>
<td></td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
</tr>
<tr>
<td></td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
Table 7: Encapsulation Support by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Physical Interface Encapsulation</th>
<th>Logical Interface Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>t3—T3 interface (including channelized OC12-to-DS3 interfaces)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cisco-hdlc—Cisco-compatible HDLC framing</td>
<td></td>
<td>frame-relay-ccc—Frame Relay DLCI for CCC</td>
</tr>
<tr>
<td>cisco-hdlc-ccc—Cisco-compatible HDLC framing for a cross-connect</td>
<td>frame-relay-ppp—PPP over Frame Relay</td>
<td>frame-relay-tcc—Frame Relay DLCI for a translational cross-connect</td>
</tr>
<tr>
<td>cisco-hdlc-tcc—Cisco-compatible HDLC framing for a translational cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>extended-frame-relay-ccc—Any Frame Relay DLCI for a cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>extended-frame-relay-tcc—Any Frame Relay DLCI for a translational cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>flexible-frame-relay—Multiple Frame Relay encapsulations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>frame-relay—Frame Relay encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>frame-relay-ccc—Frame Relay for a cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>frame-relay-port-ccc—Frame Relay port encapsulation for a cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>frame-relay-tcc—Frame Relay for a translational cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ppp—Serial PPP device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ppp-ccc—Serial PPP device for a cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ppp-tcc—Serial PPP device for a translational cross-connect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controller-level channelized IQ interfaces (cau4, coc1, coc3, coc12, cstm1, ct1, ct3, ce1)</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Services interfaces (cp, gr, ip, mo, vt, es, mo, rsp, sp)</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Unconfigurable, internally generated interfaces (gre, ipip, learning-chip (lc), lsi, tap, mt, mtun, pd, pe, pimd, pime)</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

NOTE: You can configure GRE interfaces (gre-x/y/z) only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information about GMPLS, see the MPLS Applications Feature Guide.
When you configure an interface, you are effectively specifying the properties for a physical interface descriptor. In most cases, the physical interface descriptor corresponds to a single physical device and consists of the following parts:

- The interface name, which defines the media type
- The slot in which the FPC or DPC is located
- The location on the FPC in which the PIC is installed
- The PIC or DPC port
- The interface’s channel and logical unit numbers (optional)

Each physical interface descriptor can contain one or more logical interface descriptors. These allow you to map one or more logical (or virtual) interfaces to a single physical device. Creating multiple logical interfaces is useful for ATM, Frame Relay, and Gigabit Ethernet networks, in which you can associate multiple virtual circuits, data-link connections, or virtual LANs (VLANs) with a single interface device.

Each logical interface descriptor can have one or more family descriptors to define the protocol family that is associated with and allowed to run over the logical interface.

The following protocol families are supported:

- Internet Protocol version 4 (IPv4) suite (inet)
- Internet Protocol version 6 (IPv6) suite (inet6)
- Circuit cross-connect (CCC)
- Translational cross-connect (TCC)
- International Organization for Standardization (ISO)
- Multilink Frame Relay end-to-end (MLFR end-to-end)
- Multilink Frame Relay user-to-network interface network-to-network interface (MLFR UNI NNI)
- Multilink Point-to-Point Protocol (MLPPP)
- Multiprotocol Label Switching (MPLS)
- Trivial Network Protocol (TNP)
- (M Series, T Series, and MX Series routers only) Virtual private LAN service (VPLS)
Finally, each family descriptor can have one or more address entries, which associate a
network address with a logical interface and hence with the physical interface.

You configure the various interface descriptors as follows:

- You configure the physical interface descriptor by including the `interfaces interface-name`
  statement.

- You configure the logical interface descriptor by including the `unit` statement within
  the `interfaces interface-name` statement or by including the `logical` descriptor at the
  end of the interface name, as in`t3-0/0/0.1`, where the logical unit number is 1, as shown
  in the following examples:

  ```
  [edit]
  user@host# set interfaces t3-0/0/0 unit 1
  [edit]
  user@host# edit interfaces t3-0/0/0.1
  [edit interfaces t3-0/0/0]
  user@host# set unit 1
  ```

- You configure the family descriptor by including the `family` statement within the `unit`
  statement.

- You configure address entries by including the `address` statement within the `family`
  statement.

- You configure tunnels by including the `tunnel` statement within the `unit` statement.

  **NOTE:** The address of a logical interface cannot be the same as a tunnel
  interface's source or destination address. If you try to configure a logical
  interface with a tunnel interface's address or vice versa, a commit failure will
  occur.

  Related Documentation

  - Router Interfaces Overview on page 4

**Physical Part of an Interface Name**

- Interface Names for ACX Series Universal Metro Routers on page 43
- Interface Names for M Series and T Series Routers on page 44
- MX Series Router Interface Names on page 44
- Interface Names for PTX Series Routers on page 45

**Interface Names for ACX Series Universal Metro Routers**

ACX Series routers do not have actual PIC devices. Instead they have built-in network
ports on the front panel of the router. These ports are named using the same naming
convention used for routers with PIC devices with the understanding that the FPC, PIC
and port are pseudo devices. When you display information about one of these ports,
you specify the interface type, the slot for the Flexible PIC Concentrator (FPC), the slot on the FPC for the Physical Interface Card (PIC), and the configured port number.

In the physical part of the interface name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers:

\texttt{type-fpc(pic/port)}

**See Also**

- Understanding Encapsulation on an Interface
- Configuring Inverse Multiplexing for ATM (IMA) on ACX Series

**Interface Names for M Series and T Series Routers**

On M Series and T Series routers, when you display information about an interface, you specify the interface type, the slot in which the Flexible PIC Concentrator (FPC) is installed, the slot on the FPC in which the Physical Interface Card (PIC) is located, and the configured port number.

In the physical part of the interface name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers:

\texttt{type-fpc(pic/port)}

\textbf{NOTE:} Exceptions to the \texttt{type-fpc(pic/port)} physical description include the aggregated Ethernet and aggregated SONET/SDH interfaces, which use the syntax \texttt{ae number} and \texttt{as number}, respectively.

**MX Series Router Interface Names**

On MX Series routers when you display information about an interface, you specify the interface type, the Dense Port Concentrator (DPC), Flexible PIC Concentrator (FPC), or Modular Port Concentrator (MPC) slot, the PIC or MIC slot, and the configured port number.

\textbf{NOTE:} Although the MX Series routers use DPCs, FPCs, MPCs, MICs, and PICs, command syntax in this book is shown as \texttt{fpc(pic/port)} for simplicity.

In the physical part of the interface name, a hyphen (-) separates the media type from the FPC number, and a slash (/) separates the DPC, FPC or MPC, MIC or PIC, and port numbers:

\texttt{type-fpc(pic/port)}

- \texttt{fpc}—Slot in which the DPC, FPC, or MPC is installed.
- \texttt{pic}—Slot on the FPC in which the PIC is located.
For DPCs, MICs, and the 16-port MPC, the PIC value is a logical grouping of ports and varies on different platforms.

- **port**—Port number on the DPC, PIC, MPC, or MIC.

### Interface Names for PTX Series Routers

On PTX Series Packet Transport Routers, when you display information about an interface, you specify the interface type, the slot in which the Flexible PIC Concentrator (FPC) is installed, the slot on the FPC in which the Physical Interface Card (PIC) is located, and the configured port number.

**NOTE:**

- The PTX router supports Ethernet type interfaces only. The media type portion of the physical interface name, `type`, supports the Ethernet interface type only: `et`.
- In the CLI, all PTX3000 PICs are represented as `pic0`. For more information, see [PTX3000 PIC Description](#).

In the physical part of the interface name, a hyphen (-) separates the media type (`et`) from the FPC number, and a slash (/) separates the FPC, PIC, and port numbers:

```
type-fpc/pic/port
```

**Related Documentation**

- Interface Naming Overview on page 16
- Logical Part of an Interface Name on page 23

### Displaying Interface Configurations Overview

To display a configuration, use either the `show` command in configuration mode or the `show configuration` top-level command. Interfaces are listed in numerical order, from lowest to highest slot number, then from lowest to highest PIC number, and finally from lowest to highest port number.

**Related Documentation**

- Router Interfaces Overview on page 4
CHAPTER 2

Configuring Physical Interface Properties

- Physical Interface Configuration Statements Overview on page 48
- Physical Interfaces Properties Statements List on page 58
- Configuring Interface Ranges on page 74
- Specifying an Aggregated Interface on page 84
- Media MTU Overview on page 84
- Media MTU Sizes by Interface Type on page 85
- Configuring the Media MTU on ACX Series Routers on page 94
- Encapsulation Overhead by Interface Encapsulation Type on page 97
- Configuring Interface Description on page 98
- Configuring the Media MTU on page 99
- Configuring the Interface Speed on page 100
- Configuring the Link Characteristics on page 106
- Interface Alias Names Overview on page 107
- Example: Adding an Interface Alias Name on page 108
- Clock Source Overview on page 112
- Configuring the Clock Source on page 113
- Configuring Interface Encapsulation on Physical Interfaces on page 114
- Configuring Interface Encapsulation on PTX Series Packet Transport Routers on page 117
- Configuring Keepalives on page 118
- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
- Configuring the PPP Password Authentication Protocol On a Physical Interface on page 124
- PPP Encapsulation on ACX Series Routers on page 127
- Configuring Interface Encapsulation on Physical Interfaces in ACX Series on page 129
- Configuring PPP Address and Control Field Compression on page 133
- Configuring the PPP Protocol Field Compression on page 135
- Monitoring a PPP Session on page 136
- Tracing Operations of the pppd Process on page 137
Physical Interface Configuration Statements Overview

The software driver for each network media type sets reasonable default values for general interface properties, such as the interface’s maximum transmission unit (MTU) size, receive and transmit leaky bucket properties, link operational mode, and clock source.

M Series, MX Series, and T Series routers are factory configured according to the specific router, its features, and its physical interfaces. This section includes a default configuration example showing the statements used to configure the physical interfaces properties. Additional statements are used to set properties for specific interface types and are described in “Physical Interfaces Properties Statements List” on page 58.

To modify any of the default general interface properties, include the appropriate statements at the [edit interfaces interface-name] hierarchy level:

```
interfaces {
traceoptions {
    file filename <filesnumber> <match regular-expression> <size size> <world-readable | no-world-readable >; 
    flag flag <disable>;
}
interface-name {
    accounting-profile name;
    aggregated-ether-options {

```

NOTE: The following configuration hierarchy and its included statements are shown only as an example of a configuration statement hierarchy and should not be referenced for resolving actual configurations. For information on a specific hierarchy level, see the hierarchy level document for that specific hierarchy, for example [edit interfaces] Hierarchy Level.
(flow-control | no-flow-control);
lACP {  
  (active | passive);
  link-protection{
    disable;
  (revertive | non-revertive (interfaces));
  periodic interval;
  system-priority priority;
  }
link-protection;
link-speed speed;
(loopback | no-loopback);
minimum-links number;
source-address-filter {  
  mac-address
  }
(sources-filtering | no-source-filtering);
}
aggregated-sonet-options {  
  link-speed speed | mixed;
minimum-links number;
}
atm-options {  
  cell-bundle-size cells;
  ilmi;
  linear-red-profiles profile-name {  
    high-plp-max-threshold percent;
    low-plp-max-threshold percent;
    queue-depth cells high-plp-threshold percent low-plp-threshold percent;
  }
  mpls {  
    pop-all-labels {
      required-depth number;
    }
  }
  pic-type (atm1 | atm2);
  plp-to-clp;
  promiscuous-mode {  
    vpi vpi-identifier;
  }
  scheduler-maps map-name {  
    forwarding-class class-name {  
      epd-threshold cells plp1 cells;
      linear-red-profile profile-name;
      priority (high | low);
      transmit-weight (cells number | percent number);
    }
    vc-cos-mode (alternate | strict);
  }
  vpi vpi-identifier [  
    maximum-vcs maximum-vcs;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
  }

oam-period (seconds | disable);
shaping {
  cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}
}
clocking clock-source;
data-input (system | interface interface-name);
dce;
serial-options {
  clock-rate rate;
  clocking-mode (dce | internal | loop);
  control-polarity (negative | positive);
  cts-polarity (negative | positive);
  dcd-polarity (negative | positive);
  dce-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dsr-polarity (negative | positive);
  dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dtr-circuit (balanced | unbalanced);
  dtr-polarity (negative | positive);
  encoding (nrz | nrzi);
  indication-polarity (negative | positive);
  line-protocol protocol;
  loopback mode;
  rts-polarity (negative | positive);
  tm-polarity (negative | positive);
  transmit-clock invert;
}
description text;
dialer-options {
  pool pool-name <priority priority>;
}
disable;
ds0-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  byte-encoding (nx56 | nx64);
  fcs (16 | 32);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback payload;
  start-end-flag (filler | shared);
}

e1-options {
  bert-error-rate rate;
  bert-period seconds;
  fcs (16 | 32);
  framing (g704 | g704-no-crc4 | unframed);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback (local | remote);
  start-end-flag (filler | shared);
  timeslots time-slot-range;
}

e3-options {
  atm-encapsulation (direct | plcp);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout feet;
  compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
  fcs (16 | 32);
  framing (g.751 | g.832);
  idle-cycle-flag (filler | shared);
  invert-data;
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
  start-end-flag (filler | shared);
  (unframed | no-unframed);
}

encapsulation type;

es-options {
  backup-interface es-fpc/pic/port;
}

fastether-options {
  802.3ad aex;
  (flow-control | no-flow-control);
  ignore-13-incompletes;
  ingress-rate-limit rate;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  source-address-filter {
    mac-address;
  }
}
source-filtering | no-source-filtering);
flexible-vlan-tagging;
gigether-options {
  802.3ad aex;
  (asynchronous-notification | no-asynchronous-notification);
  (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
  local-interface-offline>;
  auto-reconnect seconds;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ];
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [ values ];
      }
      output-priority-map {
        classifier {
          premium {
            forwarding-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
      policer cos-policer-name {
        aggregate {
          bandwidth-limit bps;
          burst-size-limit bytes;
        }
        premium {
          bandwidth-limit bps;
          burst-size-limit bytes;
        }
      }
    }
  }
  (gratuitous-arp-reply | no-gratuitous-arp-reply);
  hold-time up milliseconds down milliseconds;
  interface-set interface-set-name {
    interface ethernet-interface-name {
(unit unit-number [ vlan-tags-outer vlan-tag]);
}
]
isdn-options [
    bchannel-allocation (ascending | descending);
    calling-number number;
    pool pool-name <priority priority>;
    spid1 spid-string;
    spid2 spid-string;
    static-tei-val value;
    switch-type (att5e | etsi | ni1 | ntdms100 | ntt);
    t310 seconds;
    tei-option (first-call | power-up);
]
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
imi [
    lmi-type (ansi | itu | c-imi);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
]
lsq-failure-options [
    no-termination-request;
    [ trigger-link-failure interface-name ];
]
mac mac-address;
mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    cisco-interoperability send-lip-remove-link-for-link-reject;
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu | c-imi);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 seconds;
    t392 seconds;
    yellow-differential-delay milliseconds;
    encapsulation type;
]
modem-options [
    dialin (console | routable);
    init-command-string initialization-command-string;
mtu bytes;
multiservice-options {
  (core-dump | no-core-dump);
  (syslog | no-syslog);
  (dump-on-flow-control);
  flow-control-options {
    down-on-flow-control;
    dump-on-flow-control;
    reset-on-flow-control;
  }
}
native-vlan-id number;
no-gratuitous-arp-request;
no-keepalives;
no-partition {
  interface-type type;
}
optics-options {
  wavelength nm;
  alarm alarm-name {
    (syslog | link-down);
  }
  warning warning-name {
    (syslog | link-down);
  }
}
partition partition-number oc-slice oc-slice-range interface-type type;
timeslots time-slot-range;
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
  chap {
    access-profile name;
    default-chap-secret name;
    local-name name;
    passive;
  }
  compression {
    acfc;
    pfc;
  }
  dynamic-profile profile-name;
  no-termination-request;
pap {
  access-profile name;
  local-name name;
  local-password password;
  passive;
}
}
receive-bucket {
  overflow (discard | tag);
  rate percentage;
  threshold bytes;
redundancy-options {
  primary sp-fpc/pic/port;
  secondary sp-fpc/pic/port;
}
schedulers number;
serial-options {
  clock-rate rate;
  clocking-mode (dce | internal | loop);
  control-polarity (negative | positive);
  cts-polarity (negative | positive);
  dcd-polarity (negative | positive);
  dce-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dsr-polarity (negative | positive);
  dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dtr-circuit (balanced | unbalanced);
  dtr-polarity (negative | positive);
  encoding (nrz | nrzi);
  indication-polarity (negative | positive);
  line-protocol protocol;
  loopbackmode;
  rts-polarity (negative | positive);
  tm-polarity (negative | positive);
  transmit-clock invert;
}
services-options {
  inactivity-timeout seconds;
  open-timeout seconds;
  syslog {
    host hostname {
      facility-override facility-name;
      log-prefix prefix-number;
      services priority-level;
    }
  }
}
shdsl-options {
  annex (annex-a | annex-b);
  line-rate line-rate;
  loopback (local | remote);
  snr-margin {
    snext margin;
  }
}
sonet-options {
  aggregate asx;
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    preserve-interface;
    protect-circuit group-name;
    request;
    revert-time seconds;
    switching-mode (bidirectional | unidirectional);
    working-circuit group-name;
  }
  bytes {
    c2 value;
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
  }
  fcs (16 | 32);
  loopback (local | remote);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  path-trace trace-string;
  (payload-scrambler | no-payload-scrambler);
  rfc-2615;
  trigger {
    defect ignore;
    hold-time up milliseconds down milliseconds;
  }
  vtmapping (itu-t | klm);
  (z0-increment | no-z0-increment);
}
(speed (10m | 100m | 1g | auto) | speed (auto | 1Gbps | 100Mbps | 10Mbps) | speed (oc3 | oc12 | oc48));
stacked-vlan-tagging;
switch-options {
    switch-port port-number {
        (auto-negotiation | no-auto-negotiation);
        speed (10m | 100m | 1g);
        link-mode (full-duplex | half-duplex);
    }
}

multicast-statistics
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout value;
    byte-encoding (nx56 | nx64);
    crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
    crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
t3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;
    fcs (16 | 32);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    (loop-timing | no-loop-timing);
    loopback (local | payload | remote);
    (mac | no-mac);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
unidirectional;
Related Documentation

• Router Interfaces Overview on page 4

Physical Interfaces Properties Statements List

Table 8 on page 58 lists statements that you can use to configure physical interfaces.

**Table 8: Statements for Physical Interface Properties**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.3ad aex</td>
<td>Aggregated Ethernet interfaces</td>
<td>Aggregated Ethernet Interfaces Overview</td>
</tr>
<tr>
<td>access-profile name</td>
<td>Interfaces with Point-to-Point Protocol (PPP) encapsulation</td>
<td>“Configuring the PPP Challenge Handshake Authentication Protocol” on page 121</td>
</tr>
<tr>
<td>accounting-profile name</td>
<td>All</td>
<td>“Configuring Accounting for the Physical Interface” on page 156</td>
</tr>
<tr>
<td>acfc</td>
<td>Interfaces with PPP encapsulation</td>
<td>Identifying the Access Concentrator</td>
</tr>
<tr>
<td>acknowledge-retries number</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>acknowledge-timer milliseconds</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>action-red-differential-delay (disable-tx</td>
<td>remove-link)</td>
<td>Link services and voice services interfaces</td>
</tr>
<tr>
<td>advertise-interval milliseconds</td>
<td>SONET/SDH interfaces</td>
<td>Configuring APS Timers</td>
</tr>
<tr>
<td>aggregate</td>
<td>Gigabit Ethernet intelligent queuing (IQ and IQE) interfaces and Gigabit Ethernet interfaces with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>aggregate asx</td>
<td>Aggregated SONET/SDH interfaces</td>
<td>Configuring Aggregated SONET/SDH Interfaces</td>
</tr>
<tr>
<td>aggregated-ether-options</td>
<td>Aggregated Ethernet interfaces</td>
<td>Aggregated Ethernet Interfaces Overview</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate-ports</td>
<td>SONET/SDH interfaces</td>
<td>Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode</td>
</tr>
<tr>
<td>aggregated-sonet-options</td>
<td>Aggregated SONET/SDH interfaces</td>
<td>Configuring Aggregated SONET/SDH Interfaces</td>
</tr>
<tr>
<td>alarm-name</td>
<td>10-Gigabit Ethernet interfaces</td>
<td>Configuring Link Down Notification for Optics Options Alarm or Warning</td>
</tr>
<tr>
<td>alias alias-name</td>
<td>All</td>
<td>“Example: Adding an Interface Alias Name” on page 108</td>
</tr>
<tr>
<td>annex (annex-a</td>
<td>annex-b)</td>
<td>SONET interfaces using annex-b for MSP switching on M320 and M120 Routers</td>
</tr>
<tr>
<td>aps</td>
<td>SONET/SDH interfaces</td>
<td>SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td>atm-encapsulation (direct</td>
<td>plcp)</td>
<td>Configuring E3 and T3 Parameters on ATM Interfaces</td>
</tr>
<tr>
<td>atm-options</td>
<td>ATM1 and ATM2 IQ interfaces</td>
<td>&quot;Interface Encapsulations Overview&quot; on page 31</td>
</tr>
<tr>
<td>authentication-key key</td>
<td>SONET/SDH interfaces</td>
<td>SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td>bandwidth-limit bps</td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>bert-algorithm algorithm</td>
<td>E3, T1, T3, multichannel DS3, channelized interfaces (DS3, OC12, and STM1), and channelized IQ and IQE interfaces (E1 and DS3)</td>
<td>Configuring Interface Diagnostics Tools to Test the Physical Layer Connections</td>
</tr>
<tr>
<td>bert-error-rate rate</td>
<td>E1, E3, T1, T3, and channelized interfaces (DS3, OC3, OC12, and STM1)</td>
<td>Configuring Interface Diagnostics Tools to Test the Physical Layer Connections</td>
</tr>
<tr>
<td>bert-period seconds</td>
<td>E1, E3, T1, T3, and channelized interfaces (DS3, OC12, and STM1)</td>
<td>Configuring Interface Diagnostics Tools to Test the Physical Layer Connections</td>
</tr>
<tr>
<td>Configuring the T1 Buildout value</td>
<td>T1 interfaces</td>
<td>Configuring the T1 Buildout</td>
</tr>
<tr>
<td>buildout feet</td>
<td>E3 and T3 traffic over ATM interfaces</td>
<td>Configuring E3 and T3 Parameters on ATM Interfaces</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>burst-size-limit bytes</strong></td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td><strong>byte-encoding</strong> (nx56</td>
<td>nx64)</td>
<td>DSO and T1 interfaces</td>
</tr>
<tr>
<td><strong>bytes [ values</strong></td>
<td></td>
<td>SONET/SDH interfaces</td>
</tr>
<tr>
<td><strong>cbit-parity</strong></td>
<td></td>
<td>T3 interfaces</td>
</tr>
<tr>
<td><strong>cbr rate</strong></td>
<td></td>
<td>ATM interfaces</td>
</tr>
<tr>
<td><strong>cell-bundle-size cells</strong></td>
<td>ATM2 IQ interfaces using ATM Layer 2 circuit cell-relay transport mode</td>
<td>Configuring the Layer 2 Circuit Cell-Relay Cell Maximum Overview</td>
</tr>
<tr>
<td><strong>chap</strong></td>
<td></td>
<td>Interfaces with PPP encapsulation</td>
</tr>
<tr>
<td><strong>cisco-interoperability send-lip-remove-link-for-link-reject</strong></td>
<td>link services IQ (lsq) interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>classifier</strong></td>
<td></td>
<td>Gigabit Ethernet IQ interfaces</td>
</tr>
<tr>
<td><strong>clocking clock-source</strong></td>
<td></td>
<td>ATM, DSO, E1, E3, SONET/SDH, T1, and T3 interfaces</td>
</tr>
<tr>
<td><strong>clocking-mode</strong> (dce</td>
<td>internal</td>
<td>loop)</td>
</tr>
<tr>
<td><strong>clock-rate rate</strong></td>
<td></td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td><strong>compatibility-mode</strong> mode</td>
<td></td>
<td>E3 and T3 interfaces</td>
</tr>
<tr>
<td><strong>compression</strong></td>
<td></td>
<td>Interfaces with PPP encapsulation</td>
</tr>
<tr>
<td><strong>control-polarity</strong> (negative</td>
<td>positive)</td>
<td></td>
</tr>
<tr>
<td><strong>control-signal</strong> (assert</td>
<td>de-assert</td>
<td>normal)</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>core-dump</td>
<td>no-core-dump)</td>
<td>Adaptive services, monitoring services, and collector interfaces</td>
</tr>
<tr>
<td>cts (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>cts-polarity (negative</td>
<td>positive)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>dcd (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>dcd-polarity (negative</td>
<td>positive)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>dce</td>
<td>Interfaces with Frame Relay encapsulation</td>
<td>“Configuring the Router as a DCE with Frame Relay Encapsulation” on page 138</td>
</tr>
<tr>
<td>default-chap-secret name</td>
<td>Interfaces with Point-to-Point Protocol (PPP) encapsulation</td>
<td>Configuring the PPP Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>description text</td>
<td>All</td>
<td>“Configuring Interface Description” on page 98</td>
</tr>
<tr>
<td>disable</td>
<td>All</td>
<td>“Disabling a Physical Interface” on page 158 and “Tracing Operations of an Individual Router Interface” on page 335</td>
</tr>
<tr>
<td>dot1x</td>
<td>802.1x Port-Based Network Access Control</td>
<td>IEEE 802.1x Port-Based Network Access Control Overview</td>
</tr>
<tr>
<td>down-count</td>
<td>ATM interfaces</td>
<td>Configuring the ATM OAM FS Loopback Cell Threshold</td>
</tr>
<tr>
<td>drop-timeout milliseconds</td>
<td>Multilink, link services, and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>ds0-options</td>
<td>DS0 interfaces</td>
<td>Channelized Interfaces Overview</td>
</tr>
<tr>
<td>dsr (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>dsr-polarity (negative</td>
<td>positive)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>dte-options</td>
<td>Serial interfaces (EIA-530, V.35, and X.21) on M Series and T Series routers</td>
<td>“Configuring the Serial Signal Handling” on page 324</td>
</tr>
</tbody>
</table>
Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dtr signal-handling-option</code></td>
<td>Serial interfaces (EIA-530 and V.35)</td>
<td>“Configuring the Serial Signal Handling” on page 324</td>
</tr>
<tr>
<td>`dtr-circuit (balanced</td>
<td>unbalanced)`</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>`dtr-polarity (negative</td>
<td>positive)`</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td><code>e1-options</code></td>
<td>E1 interfaces</td>
<td>E1 Interfaces Overview</td>
</tr>
<tr>
<td><code>e3-options</code></td>
<td>E3 interfaces</td>
<td>E3 Interfaces Overview</td>
</tr>
<tr>
<td><code>encapsulation type</code></td>
<td>All interfaces, except loopback and multicast tunnel</td>
<td>“Configuring Interface Encapsulation on Physical Interfaces” on page 114</td>
</tr>
<tr>
<td>`encoding (nrz</td>
<td>nrzi)`</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
</tr>
<tr>
<td><code>epd-threshold cells</code></td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td><code>es-options</code></td>
<td>ES interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><code>ethernet-policer-profile</code></td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC, and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td><code>ethernet-switch-profile</code></td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC, Aggregated Ethernet with Gigabit Ethernet IQ interfaces, and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers, Configuring MAC Address Filtering, and Configuring the Management Ethernet Interface</td>
</tr>
<tr>
<td><code>facility-override facility-name</code></td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><code>fastether-options</code></td>
<td>Fast Ethernet interfaces</td>
<td>Ethernet Interfaces Overview</td>
</tr>
<tr>
<td>`fcs (16</td>
<td>32)`</td>
<td>E1/E3, SONET/SDH, and T1/T3 interfaces</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>feac-loop-respond</td>
<td>T3 interfaces</td>
<td>Configuring the T3 FEAC Response</td>
</tr>
<tr>
<td>no-feac-loop-respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>flow-control</td>
<td>Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces</td>
<td>Configuring Flow Control</td>
</tr>
<tr>
<td>no-flow-control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>force</td>
<td>SONET/SDH interfaces</td>
<td>Configuring Switching Between the Working and Protect Circuits</td>
</tr>
<tr>
<td>forwarding-class class-name</td>
<td>ATM2 IQ interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>forwarding-class</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>fragment-threshold bytes</td>
<td>Multilink, link services, and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>framing framing-type</td>
<td>E1, E3, and T1 interfaces</td>
<td>Configuring E3 and T3 Parameters on ATM Interfaces, Configuring E1 Framing, and Configuring T1 Framing</td>
</tr>
<tr>
<td>framing</td>
<td>10-Gigabit Ethernet interfaces</td>
<td>Framing Overview</td>
</tr>
<tr>
<td>gigether-options</td>
<td>Gigabit Ethernet and Tri-Rate Ethernet copper interfaces</td>
<td>Ethernet Interfaces Overview</td>
</tr>
<tr>
<td>(gratuitous-arp-reply</td>
<td>Ethernet interfaces</td>
<td>Configuring Gratuitous ARP</td>
</tr>
<tr>
<td>no-gratuitous-arp-reply)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hello-timer milliseconds</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>high-pip-max-threshold</td>
<td>ATM2 interfaces</td>
<td>Configuring ATM2 IQ VC Tunnel CoS Components</td>
</tr>
<tr>
<td>high-pip-threshold percent</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>hold-time milliseconds</td>
<td>SONET/SDH interfaces</td>
<td>SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td>hold-time up milliseconds down milliseconds</td>
<td>All interfaces, except aggregated SONET/SDH, generalized routing encapsulation (GRE) tunnel, and IP tunnel</td>
<td>Configuring SONET/SDH Defect Triggers</td>
</tr>
<tr>
<td>host hostname</td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ieee802.1p premium [values]</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Specifying an Input Priority Map</td>
</tr>
<tr>
<td>idle-cycle-flag value</td>
<td>E1, E3, T1, and T3 interfaces</td>
<td>Configuring the E1 Idle Cycle Flag, Configuring the E3 Idle Cycle Flag, Configuring the T1 Idle Cycle Flag, and Configuring the T3 Idle Cycle Flag</td>
</tr>
<tr>
<td>ignore-all</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configuring the Serial Signal Handling” on page 324</td>
</tr>
<tr>
<td>ilmi</td>
<td>ATM interfaces</td>
<td>Configuring Communication with Directly Attached ATM Switches and Routers</td>
</tr>
<tr>
<td>inactivity-timeout seconds</td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>indication (ignore</td>
<td>normal</td>
<td>require)</td>
</tr>
<tr>
<td>indication-polarity (negative</td>
<td>positive)</td>
<td>Serial interfaces (X.21)</td>
</tr>
<tr>
<td>ingress-rate-limit rate</td>
<td>8-port, 12-port, and 48-port Fast Ethernet interfaces</td>
<td>Configuring the Ingress Rate Limit</td>
</tr>
<tr>
<td>input-priority-map</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Specifying an Input Priority Map</td>
</tr>
<tr>
<td>interface-type type</td>
<td>Channelized IQ and IQE interfaces</td>
<td>Channelized Interfaces Overview</td>
</tr>
<tr>
<td>invert-data</td>
<td>DS0, E1, E3, and T1 interfaces</td>
<td>Configuring E1 Data Inversion, Configuring E3 Data Inversion, and Configuring T1 Data Inversion</td>
</tr>
<tr>
<td>keepalives &lt;down-count number &lt;interval seconds&gt; &lt;up-count number&gt;</td>
<td>Aggregated SONET/SDH, DS0, E1, E3, SONET/SDH, T1, and T3 interfaces</td>
<td>“Configuring Keepalives” on page 118</td>
</tr>
<tr>
<td>lacp mode</td>
<td>Aggregated Ethernet interfaces</td>
<td>Configuring LACP for Aggregated Ethernet Interfaces</td>
</tr>
<tr>
<td>line-encoding (ami</td>
<td>b8zs)</td>
<td>T1 interfaces</td>
</tr>
<tr>
<td>line-protocol protocol</td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configuring the Serial Line Protocol” on page 318</td>
</tr>
<tr>
<td>linear-red-profile profile-name</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>linear-red-profiles profile-name</td>
<td>ATM2 interfaces</td>
<td>ATM2 QoS VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>link-layer-overhead percent</td>
<td>AS PIC link services IQ interfaces (lsq)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>link-mode mode</td>
<td>Management Ethernet (fxp0 or em0) and Fast Ethernet interfaces</td>
<td>“Configuring the Link Characteristics” on page 106, “Understanding Management Ethernet Interfaces” on page 10</td>
</tr>
<tr>
<td>link-speed speed</td>
<td>Aggregated Ethernet interfaces</td>
<td>“Configuring Aggregated Ethernet Link Speed” on page 102</td>
</tr>
<tr>
<td>link-speed speed</td>
<td>Aggregated SONET/SDH interfaces</td>
<td>Configuring Aggregated SONET/SDH Interfaces</td>
</tr>
<tr>
<td>lmi lmi-options</td>
<td>Interfaces with Frame Relay encapsulation</td>
<td>Configuring Frame Relay Keepalives and Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>lmi</td>
<td>OAM CFM Ethernet Local Management Interface</td>
<td>Configuring Ethernet Local Management Interface</td>
</tr>
<tr>
<td>lmi-type (ansi</td>
<td>itu</td>
<td>c-lmi)</td>
</tr>
<tr>
<td>local-name name</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Challenge Handshake Authentication Protocol” on page 121</td>
</tr>
<tr>
<td>lockout</td>
<td>SONET/SDH interfaces</td>
<td>Configuring Lockout of Protection for SDH Interfaces</td>
</tr>
<tr>
<td>log-prefix prefix-number</td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>(long-buildout</td>
<td>no-long-buildout)</td>
<td>T3 interfaces</td>
</tr>
<tr>
<td>(loop-timing</td>
<td>no-loop-timing)</td>
<td>Channelized IQ interfaces</td>
</tr>
<tr>
<td>loopback mode</td>
<td>DS0, E1, E3, T1, T3, SHDSL on ATM and SONET/SDH interfaces</td>
<td>Configuring E1 Loopback Capability, Configuring E3 Loopback Capability, Configuring T1 Loopback Capability, Configuring T3 Loopback Capability, Configuring SHDSL Operating Mode on an ATM Physical Interface, Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External, and Configuring Ethernet Loopback Capability</td>
</tr>
</tbody>
</table>
Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>loopback</strong> mode</td>
<td>Ethernet and 10-Gigabit Ethernet interfaces in WAN PHY mode</td>
<td>Configuring Ethernet Loopback Capability</td>
</tr>
<tr>
<td><strong>loopback</strong> mode</td>
<td>Serial interfaces</td>
<td>“Configuring Serial Loopback Capability” on page 328</td>
</tr>
<tr>
<td>(loopback</td>
<td>no-loopback)</td>
<td>Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces</td>
</tr>
<tr>
<td>loss-priority (high</td>
<td>low)</td>
<td>Gigabit Ethernet IQ interfaces</td>
</tr>
<tr>
<td>lowest-priority-defect (all-defects</td>
<td>err-xcon</td>
<td>mac-rem-err-xcon</td>
</tr>
<tr>
<td>low-plp-max-threshold percent</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>low-plp-threshold percent</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>lsq-failure-options</td>
<td>Link services IQ (lsq) interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>Management Ethernet interface (fpx0 or em0)</td>
<td>Configuring the MAC Address on the Management Ethernet Interface, “Understanding Management Ethernet Interfaces” on page 10</td>
</tr>
<tr>
<td>(mac-learn-enable</td>
<td>no-mac-learn-enable)</td>
<td>Gigabit Ethernet IQ and IQE, Tri-Rate Ethernet copper, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
</tr>
<tr>
<td>master-only;</td>
<td>Management Ethernet (fpx0 or em0) and Fast Ethernet interfaces</td>
<td>Configuring a Consistent Management IP Address, “Understanding Management Ethernet Interfaces” on page 10</td>
</tr>
<tr>
<td>maximum-vcs maximum-vcs</td>
<td>ATM interfaces</td>
<td>Configuring the Maximum Number of ATM1 VCs on a VP</td>
</tr>
<tr>
<td>mc-ae</td>
<td>Aggregated Ethernet interfaces</td>
<td>Configuring Multichassis Link Aggregation on MX Series Routers</td>
</tr>
<tr>
<td>minimum-links number</td>
<td>Multilink, link services, and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>mip-half-function</td>
<td>Connectivity Fault Management</td>
<td>Configuring IEEE 802.3ah OAM Link-Fault Management</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>mlfr-uni-nni-bundle-options</em></td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>mpls</em></td>
<td>10-Gigabit Ethernet interfaces in WAN PHY mode and ATM and SONET/SDH interfaces in passive monitoring mode</td>
<td>Removing MPLS Labels from Incoming Packets, Enabling Packet Flow Monitoring on SONET/SDH Interfaces, and SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>mrru</em> bytes</td>
<td>Link services and voice services interfaces</td>
<td>Junos Services Interfaces Configuration Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>mtu</em> bytes</td>
<td>All interfaces, except management Ethernet (<em>fxp0</em> or <em>em0</em>), loopback, multilink, and multicast tunnel</td>
<td>&quot;Understanding Management Ethernet Interfaces&quot; on page 10, &quot;Media MTU Overview&quot; on page 84, &quot;Configuring the Media MTU&quot; on page 99</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>multicast-statistics</em></td>
<td>Ethernet, SONET, aggregated Ethernet, and aggregated SONET interfaces.</td>
<td>Configuring Multicast Statistics Collection on Aggregated Ethernet Interfaces, Configuring Multicast Statistics Collection on SONET Interfaces, Configuring Multicast Statistics Collection on Ethernet Interfaces, and Configuring Multicast Statistics Collection on Aggregated SONET Interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>multiservice-options</em></td>
<td>Adaptive services, monitoring services, and collector interfaces</td>
<td>&quot;Configuring Multiservice Physical Interface Properties&quot; on page 154</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>n391</em> number</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>n392</em> number</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>n393</em> number</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>neighbor</em> address</td>
<td>SONET/SDH interfaces</td>
<td>SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>no-gratuitous-arp-request</em></td>
<td>Ethernet interfaces</td>
<td>Configuring Gratuitous ARP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>no-keepalives</em></td>
<td>Interfaces with PPP, Frame Relay, or Cisco High-level Data Link Control (HDLC) encapsulation</td>
<td>&quot;Configuring Keepalives&quot; on page 118</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>no-partition</em></td>
<td>Channelized IQ interfaces</td>
<td>Channelized Interfaces Overview</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>no-termination-request</em></td>
<td>Link Services IQ (LSQ) interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>oam-liveness</td>
<td>ATM interfaces</td>
<td>Configuring the OAM F4 Cell Flows</td>
</tr>
<tr>
<td>oam-period</td>
<td>ATM interfaces</td>
<td>Defining the ATM OAM F5 Loopback Cell Period</td>
</tr>
<tr>
<td>oc-slice</td>
<td>Channelized OC12 IQ interfaces</td>
<td>Channelized OC12/STM4 IQ and IQE Interfaces Overview</td>
</tr>
<tr>
<td>open-timeout</td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>optics-options</td>
<td>Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces</td>
<td>Ethernet DWDM Interface Wavelength Overview</td>
</tr>
<tr>
<td>output-priority-map</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>overflow</td>
<td>All interfaces, except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ interfaces</td>
<td>“Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion” on page 140</td>
</tr>
<tr>
<td>paired-group</td>
<td>SONET/SDH interfaces</td>
<td>Configuring APS Load Sharing</td>
</tr>
<tr>
<td>partition</td>
<td>Channelized IQ interfaces</td>
<td>Channelized Interfaces Overview</td>
</tr>
<tr>
<td>passive</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Challenge Handshake Authentication Protocol” on page 121</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>SONET/SDH interfaces</td>
<td>Enabling Packet Flow Monitoring on SONET/SDH Interfaces</td>
</tr>
<tr>
<td>path-trace</td>
<td>10-Gigabit Ethernet interfaces in WAN PHY mode and SONET/SDH interfaces</td>
<td>Configuring the SONET/SDH Path Trace Identifier for a Circuit</td>
</tr>
<tr>
<td>(payload-scrambler</td>
<td>E3, SONET/SDH, and T3 interfaces</td>
<td>Configuring E3 and T3 Parameters on ATM Interfaces, Configuring E3 HDLC Payload Scrambling, Configuring SONET/SDH HDLC Payload Scrambling for Link Stability, and Configuring T3 HDLC Payload Scrambling</td>
</tr>
<tr>
<td>periodic</td>
<td>Aggregated Ethernet interfaces</td>
<td>Configuring LACP for Aggregated Ethernet Interfaces</td>
</tr>
<tr>
<td>per-unit-scheduler</td>
<td>IQ interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>pfc</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Protocol Field Compression” on page 135</td>
</tr>
<tr>
<td>pic-type (atm1</td>
<td>atm2)</td>
<td>ATM2 IQ interfaces</td>
</tr>
<tr>
<td>plp1 cells</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>plp-to-clp</td>
<td>ATM2 IQ interfaces</td>
<td>Enabling the PLP Setting to Be Copied to the CLP Bit</td>
</tr>
<tr>
<td>policer cos-policer-name</td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>pop-all-labels</td>
<td>ATM and SONET/SDH interfaces in passive monitoring mode</td>
<td>Removing MPLS Labels from Incoming Packets and Enabling Packet Flow Monitoring on SONET/SDH Interfaces</td>
</tr>
<tr>
<td>ppp-options</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Challenge Handshake Authentication Protocol” on page 121</td>
</tr>
<tr>
<td>premium</td>
<td>Enhanced Intelligent Queuing (IQE) interfaces (hierarchical policer)</td>
<td>“Applying Policers” on page 210 and Class of Service Feature Guide (Routers and EX9200 Switches)</td>
</tr>
<tr>
<td>premium</td>
<td>Gigabit Ethernet IQ interfaces (policer)</td>
<td>Configuring Gigabit Ethernet Policers</td>
</tr>
<tr>
<td>premium</td>
<td>Gigabit Ethernet IQ interfaces (output priority map)</td>
<td>Configuring MAC Address Filtering</td>
</tr>
<tr>
<td>primary sp-fpc/pic/port</td>
<td>Redundant interfaces for adaptive services interfaces (rsp-)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>priority (high</td>
<td>low)</td>
<td>ATM2 IQ interfaces</td>
</tr>
<tr>
<td>priority number</td>
<td>Ethernet protocols (OAM CFM)</td>
<td>Configuring a MEP to Generate and Respond to CFM Protocol Messages</td>
</tr>
<tr>
<td>promiscuous-mode</td>
<td>ATM2 IQ interfaces</td>
<td>Configuring ATM Cell-Relay Promiscuous Mode</td>
</tr>
<tr>
<td>protect-circuit group-name</td>
<td>SONET/SDH interfaces</td>
<td>Configuring Switching Between the Working and Protect Circuits</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>queue-depth cells</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>queue-length number</td>
<td>ATM1 interfaces</td>
<td>Configuring the ATMI Queue Length</td>
</tr>
<tr>
<td>rate percentage</td>
<td>All interfaces, except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ</td>
<td>“Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion” on page 140</td>
</tr>
<tr>
<td>receive-bucket</td>
<td>All interfaces, except ATM, Fast Ethernet, and Gigabit Ethernet</td>
<td>“Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion” on page 140</td>
</tr>
<tr>
<td>red-differential-delay milliseconds</td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>redundancy-options</td>
<td>Redundant interfaces for adaptive services interfaces (rsp-)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>remote-loopback-respond</td>
<td>T1 interfaces</td>
<td>Configuring the T1 Remote Loopback Response</td>
</tr>
<tr>
<td>request</td>
<td>SONET/SDH interfaces</td>
<td>Configuring Switching Between the Working and Protect Circuits</td>
</tr>
<tr>
<td>required-depth number</td>
<td>ATM and SONET/SDH interfaces in passive monitoring mode</td>
<td>Removing MPLS Labels from Incoming Packets and Enabling Packet Flow Monitoring on SONET/SDH Interfaces</td>
</tr>
<tr>
<td>revert-time seconds</td>
<td>SONET/SDH interfaces</td>
<td>Configuring Revertive Mode</td>
</tr>
<tr>
<td>rfc-2615</td>
<td>SONET/SDH interfaces</td>
<td>Configuring PPP Support on SONET/SDH Interfaces</td>
</tr>
<tr>
<td>rts (assert</td>
<td>de-assert</td>
<td>normal)</td>
</tr>
<tr>
<td>rts-polarity (negative</td>
<td>positive)</td>
<td>Serial interfaces (EIA-530 and V.35)</td>
</tr>
<tr>
<td>rtvbr</td>
<td>ATM interfaces</td>
<td>Configuring ATM CBR</td>
</tr>
<tr>
<td>scheduler-maps map-name</td>
<td>ATM2 interfaces</td>
<td>ATM2 IQ VC Tunnel CoS Components Overview</td>
</tr>
<tr>
<td>schedulers number</td>
<td>Ethernet IQ2 and IQ2-E PICs port interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>secondary sp-fpc/pic/port</code></td>
<td>Redundant interfaces for adaptive services interfaces (<code>rsp-</code>)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><code>services-options</code></td>
<td>Services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><code>serial-options</code></td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Serial Interfaces Overview” on page 315</td>
</tr>
<tr>
<td><code>services priority-level</code></td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><code>size</code></td>
<td>All</td>
<td>“Tracing Operations of the Interface Process” on page 336</td>
</tr>
<tr>
<td><code>shaping</code></td>
<td>ATM interfaces</td>
<td>Defining the ATM Traffic-Shaping Profile Overview</td>
</tr>
<tr>
<td><code>shaping</code></td>
<td>Circuit Emulation PICs</td>
<td>Configuring ATM QoS or Shaping</td>
</tr>
<tr>
<td><code>sonet-options</code></td>
<td>SONET/SDH interfaces</td>
<td>SONET/SDH Interfaces Overview</td>
</tr>
<tr>
<td><code>source-address-filter mac-address</code></td>
<td>Aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, and Gigabit Ethernet interfaces</td>
<td>Configuring MAC Address Filtering for Ethernet Interfaces</td>
</tr>
<tr>
<td>`(source-filtering</td>
<td>no-source-filtering)`</td>
<td>Aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet IQ and IQE, and Gigabit Ethernet interfaces with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
</tr>
<tr>
<td>`speed (10m</td>
<td>100m</td>
<td>1g</td>
</tr>
<tr>
<td>`speed (oc3</td>
<td>oc12</td>
<td>oc48)`</td>
</tr>
<tr>
<td><code>stacked-vlan-tagging</code></td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview</td>
</tr>
<tr>
<td>`start-end-flag (filler</td>
<td>shared)`</td>
<td>DS0, E1, E3, T1, and T3 interfaces</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>switching-mode</strong></td>
<td>Unchannelized OC3, OC12, and OC48 SONET/SDH interfaces on T Series routers</td>
<td><strong>Configuring Switching Mode</strong></td>
</tr>
<tr>
<td><strong>syslog</strong></td>
<td>Adaptive services interfaces</td>
<td><strong>Junos OS Services Interfaces Library for Routing Devices</strong></td>
</tr>
<tr>
<td>**(syslog</td>
<td>no-syslog)**</td>
<td>Adaptive services, monitoring services, and collector interfaces</td>
</tr>
<tr>
<td><strong>t1-options</strong></td>
<td>T1 interfaces</td>
<td><strong>T1 Interfaces Overview</strong></td>
</tr>
<tr>
<td><strong>t3-options</strong></td>
<td>T3 interfaces</td>
<td><strong>T3 Interfaces Overview</strong></td>
</tr>
<tr>
<td><strong>t391 seconds</strong></td>
<td>Link services and voice services interfaces</td>
<td><strong>Junos OS Services Interfaces Library for Routing Devices</strong></td>
</tr>
<tr>
<td><strong>t392 number</strong></td>
<td>Link services and voice services interfaces</td>
<td><strong>Junos OS Services Interfaces Library for Routing Devices</strong></td>
</tr>
<tr>
<td><strong>threshold bytes</strong></td>
<td>All interfaces, except ATM, channelized E1, E1, Fast Ethernet, Gigabit Ethernet, and channelized IQ</td>
<td>“Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion” on page 140</td>
</tr>
<tr>
<td><strong>timeslots time-slot-range</strong></td>
<td>Channelized T1 IQ and channelized E1 IQ interfaces</td>
<td><strong>Channelized Interfaces Overview</strong></td>
</tr>
<tr>
<td>**tm (ignore</td>
<td>normal</td>
<td>require)**</td>
</tr>
<tr>
<td>**tm-polarity (negative</td>
<td>positive)**</td>
<td>Serial interfaces (EIA-530)</td>
</tr>
<tr>
<td><strong>traceoptions</strong></td>
<td>All</td>
<td>“Tracing Operations of an Individual Router Interface” on page 335</td>
</tr>
<tr>
<td><strong>traceoptions</strong></td>
<td>All</td>
<td>“Tracing Operations of the Interface Process” on page 336</td>
</tr>
<tr>
<td><strong>transmit-bucket</strong></td>
<td>All interfaces, except ATM, Fast Ethernet, Tri-Rate Ethernet copper, and Gigabit Ethernet</td>
<td>“Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion” on page 140</td>
</tr>
<tr>
<td><strong>transmit-clock invert</strong></td>
<td>Serial interfaces (EIA-530, V.35, and X.21)</td>
<td>“Configuring the Serial Clocking Mode” on page 322</td>
</tr>
<tr>
<td>**transmit-weight (cells number</td>
<td>percent number)**</td>
<td>ATM2 IQ interfaces</td>
</tr>
</tbody>
</table>
### Table 8: Statements for Physical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>(traps</td>
<td>All</td>
<td>“Enabling or Disabling SNMP Notifications on Physical Interfaces” on page 155</td>
</tr>
<tr>
<td>no-traps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>trigger `defect ignore</td>
<td>defect hold-time up milliseconds down milliseconds;`</td>
<td>10-Gigabit Ethernet interfaces in WAN PHY mode and ATM over SONET/SDH and SONET/SDH interfaces</td>
</tr>
<tr>
<td>`(unframed</td>
<td>All</td>
<td>Configuring E3 IQ and IQE Unframed Mode</td>
</tr>
<tr>
<td>no-unframed)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unidirectional</td>
<td>10-Gigabit Ethernet interfaces on:</td>
<td>“Enabling Unidirectional Traffic Flow on Physical Interfaces” on page 142</td>
</tr>
<tr>
<td></td>
<td>• MX960 4–Port 10–Gigabit Ethernet DPC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T Series 10–Gigabit Ethernet IQ2 PIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T Series 10–Gigabit Ethernet IQ2E PIC</td>
<td></td>
</tr>
<tr>
<td><code>vbr peak rate sustained rate burst length</code></td>
<td>ATM interfaces</td>
<td>Defining the ATM Traffic-Shaping Profile Overview</td>
</tr>
<tr>
<td>`vc-cos-mode (alternate</td>
<td>strict)`</td>
<td>ATM2 interfaces</td>
</tr>
<tr>
<td><code>vlan-tagging</code></td>
<td>Fast Ethernet, Tri-Rate Ethernet copper, and Gigabit Ethernet interfaces</td>
<td>802.1Q VLANs Overview</td>
</tr>
<tr>
<td><code>vlan-vci-tagging</code></td>
<td>Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet interfaces</td>
<td>“Configuring ATM-to-Ethernet Interworking” on page 262</td>
</tr>
<tr>
<td><code>vpi vpi-identifier</code></td>
<td>ATM interfaces</td>
<td>Configuring ATM Cell-Relay Promiscuous Mode and Configuring the Maximum Number of ATM1 VCs on a VP</td>
</tr>
<tr>
<td><code>vtnmapping</code></td>
<td>Channelized STM1 interfaces</td>
<td>Configuring Virtual Tributary Mapping of Channelized STM1 Interfaces</td>
</tr>
<tr>
<td>`warning warning-name (syslog</td>
<td>link-down)`</td>
<td>10-Gigabit Ethernet interfaces</td>
</tr>
<tr>
<td><code>wavelength nm</code></td>
<td>Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces</td>
<td>Ethernet DWDM Interface Wavelength Overview</td>
</tr>
<tr>
<td><code>working-circuit group-name</code></td>
<td>SONET/SDH interfaces</td>
<td>Configuring Switching Between the Working and Protect Circuits</td>
</tr>
<tr>
<td><code>yellow-differential-delay milliseconds</code></td>
<td>Link services and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
</tbody>
</table>
Configuring Interface Ranges

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 Interface Ranges for EX Series Switches with ELS. For ELS details, see Using the Enhanced Layer 2 Software CLI.

The Junos OS allows you to group a range of identical interfaces into an *interface range*. You first specify the group of identical interfaces in the interface range. Then you can apply a common configuration to the specified interface range, reducing the number of configuration statements required and saving time while producing a compact configuration.

- Configuring Interface Ranges on page 74
- Expanding Interface Range Member and Member Range Statements on page 78
- Configuration Inheritance for Member Interfaces on page 80
- Member Interfaces Inheriting Configuration from Configuration Groups on page 81
- Interfaces Inheriting Common Configuration on page 82
- Configuring Inheritance Range Priorities on page 82
- Configuration Expansion Where Interface Range Is Used on page 83

### Configuring Interface Ranges

To configure an interface range, include the `interface-range` statement at the [edit interfaces] hierarchy level.

The `interface-range` statement accepts only physical networking interface names in its definition. The following interface types are supported and example CLI descriptors are shown:

- ATM—`at-fpc/pic/port`
- Channelized—`(coc | cstm)n-fpc/pic/port`
- DPC—`xe-fpc/pic/port`
Interfaces can be grouped either as a range of interfaces or using a number range under the interface-range statement definition.

Interfaces in an interface-range definition can be added as part of a member range or as individual members or multiple members using a number range.

To specify a member range, use the member-range statement at the [edit interfaces interface-range name] hierarchy level.

To specify interfaces in lexical order, use the member-range start-range to end-range statement.

A range for a member statement should contain the following:

- *—All, specifies sequential interfaces from 0 through 47.

  **CAUTION:** The wildcard * in a member statement does not take into account the interface numbers supported by a specific interface type. Irrespective of the interface type, * includes interface numbers ranging from 0 through 47 to the interface group. Therefore, use * in a member statement with caution.

- num—Number, specifies one specific interface by its number.

- [low-high]—Numbers between low to high, specifies a range of sequential interfaces.

- [num1, num2, num3]—Numbers num1, num2, and num3 specify multiple specific interfaces.

**Example: Specifying an Interface Range Member Range**

```plaintext
member-range ge-0/0/0 to ge-4/0/40;
```

To specify one or multiple members, use the member statement at the [edit interfaces interface-range name] hierarchy level.

To specify the list of interface range members individually or for multiple interfaces using regex, use the member list of interface names statement.
Example: Specifying an Interface Range Member

member ge-0/0/0;
member ge-0/*/*
member ge-0/[1-10]/0;
member ge-0/[1,2,3]/3;

Regex or wildcards are not supported for interface-type prefixes. For example, prefixes ge, fe, and xe must be mentioned explicitly.

An interface-range definition can contain both member and member-range statements within it. There is no maximum limit on the number of member or member-range statements within an interface-range. However, at least one member or member-range statement must exist within an interface-range definition.

Example: Interface Range Common Configuration

Configuration common to an interface range can be added as a part of the interface-range definition, as follows:

[edit]
interfaces {
    + interface-range foo {
        + member-range ge-1/0/0 to ge-4/0/40;
        + member ge-0/1/1;
        + member ge-5/[1-10]/4;
        /*Common configuration is added as part of interface-range definition*/
        mtu 256;
        hold-time up 10;
        ether-options {
            flow-control;
            speed {
                100m;
            }
            802.3ad primary;
        }
    }
}

An interface-range definition having just member or member-range statements and no common configurations statements is valid.

These defined interface ranges can be used in other configuration hierarchies, in places where an interface node exists.

Example: Interface-Range foo Used Under the Protocols Hierarchy

protocols {
    dot1x {
        authenticator {
            interface foo{
                retries 1;
            }
        }
    }
}
foo should be an `interface-range` defined at the `[interfaces]` hierarchy level. In the above example, the `interface` node can accept both individual interfaces and interface ranges.

**TIP:** To view an interface range in expanded configuration, use the `(show | display inheritance)` command. For more information, see the *CLI User Guide*.

By default, `interface-range` is not available to configure in the CLI where the `interface` statement is available. The following locations are supported; however, some of the hierarchies shown in this list are product specific:

- `protocols dot1x authentication interface`
- `protocols dvmrp interface`
- `protocols oam ethernet lmi interface`
- `protocols esis interface`
- `protocols igmp interface`
- `protocols igmp-host client num interface`
- `protocols mid-host client num interface`
- `protocols router-advertisement interface`
- `protocols isis interface`
- `protocols ldp interface`
- `protocols oam ethernet link-fault-management interface`
- `protocols ldp interface`
- `protocols link-management peer lmp-control-channel interface`
- `protocols link-management peer control-channel`
- `protocols link-management te-link name interface`
- `protocols mld interface`
- `protocols ospf area id interface`
- `protocols pim interface`
- `protocols router-discovery interface`
- `protocols rip group name neighbour`
- `protocols ripng group name neighbour`
- `protocols rsvp interface`
- `protocols snmp interface`
- `protocols layer2-control bpdu-block interface`
- `protocols layer2-control mac-rewrite interface`
• protocols mpls interface
• protocols stp interface
• protocols rstp interface
• protocols mstp interface
• protocols vstp interface
• protocols mstp msti id interface
• protocols mstp msti vlan id interface
• protocols vstp vlan name interface
• protocols gvrp interface
• protocols igmp-snooping vlan name interface
• protocols lldp interface
• protocols lldp-med interface
• protocols sflow interfaces
• ethernet-switching-options analyzer name input [egress | ingress] interface
• ethernet-switching-options analyzer name output interface
• ethernet-switching-options secure-access-port interface
• ethernet-switching-options interfaces ethernet-switching-options voip interface
• ethernet-switching-options interfaces ethernet-switching-options redundant-trunk-group group g1 interface
• ethernet-switching-options redundant-trunk-group group g1 interface
• ethernet-switching-options bpdu-block interface
• poe interface vlans pro-bng-mcl-bsd1 interface

See Also

• Expanding Interface Range Member and Member Range Statements
• Configuration Inheritance for Member Interfaces
• Member Interfaces Inheriting Configuration from Configuration Groups
• Interfaces Inheriting Common Configuration
• Configuring Inheritance Range Priorities
• Configuration Expansion Where Interface Range Is Used
• Physical Interfaces

Expanding Interface Range Member and Member Range Statements

All member and member-range statements in an interface range definition are expanded to generate the final list of interface names for the specified interface range.
Example: Expanding Interface Range Member and Member Range Statements

[edit]
interfaces {
  interface-range range-1 {
    member-range ge-0/0/0 to ge-4/0/20;
    member ge-10/1/1;
    member ge-5/[0-5]/*;
    /*Common configuration is added part of the interface-range definition*/
    mtu 256;
    hold-time up 10;
    ether-options {
      flow-control;
      speed {
        100m;
      }
      802.3ad primary;
    }
  }
}

For the member-range statement, all possible interfaces between start-range and end-range are considered in expanding the members. For example, the following member-range statement:

member-range ge-0/0/0 to ge-4/0/20

expands to:

[ge-0/0/0, ge-0/0/1 ... ge-0/0/max_ports
 ge-0/1/0 ge-0/1/1 ... ge-0/1/max_ports
 ge-0/2/0 ge-0/2/1 ... ge-0/2/max_ports
   ...
 ge-0/MAX_PICS/0 ... ge-0/max_pics/max_ports
 ge-1/0/0 ge-1/0/1 ... ge-1/0/max_ports
   ...
 ge-1/MAX_PICS/0 ... ge-1/max_pics/max_ports
   ...
 ge-4/0/0 ge-4/0/1 ... ge-4/0/max_ports]

The following member statement:

ge-5/[0-5]/*

expands to:

ge-5/0/0 ... ge-5/0/max_ports
ge-5/1/0 ... ge-5/0/max_ports
  ...
ge-5/5/0 ... ge-5/5/max_ports

The following member statement:
**Configuration Inheritance for Member Interfaces**

When the Junos OS expands the `member` and `member-range` statements present in an `interface-range`, it creates interface objects if they are not explicitly defined in the configuration. The common configuration is copied to all its member interfaces in the `interface-range`.

**Example:**

Foreground interface configuration takes priority compared to configuration inherited by the interface through the `interface-range`.

```
interfaces {
  interface-range range-1 {
    member-range ge-1/0/0/0 to ge-10/0/47;
    mtu 256;
  }
  ge-1/0/1 {
    mtu 1024;
  }
}
```

In the preceding example, interface `ge-1/0/1` will have an MTU value of 1024.

This can be verified with output of the `show interfaces | display inheritance` command, as follows:

```
user@host: # show interfaces | display inheritance
## 'ge-1/0/0' was expanded from interface-range 'range-1'
##
ge-1/0/0 {
  ## '256' was expanded from interface-range 'range-1'
  ##
  mtu 256;
}
ge-1/0/1 {
  mtu 1024;
}
##
## 'ge-1/0/2' was expanded from interface-range 'range-1'
##
ge-1/0/2 {
  ## '256' was expanded from interface-range 'range-1'
  ##
  mtu 256;
}
```
Member Interfaces Inheriting Configuration from Configuration Groups

Interface range member interfaces inherit the config-groups configuration like any other foreground configuration. `interface-range` is similar to any other foreground configuration statement. The only difference is that the `interface-range` goes through a member interfaces expansion before Junos OS reads this configuration.

groups {
    global {
        interfaces {
            <*> {
                hold-time up 10;
            }
        }
    }
}
apply-groups [global];
interfaces {
    interface-range range-1 {
        member-range ge-1/0/0 to ge-10/0/47;
        mtu 256;
    }
}

The `hold-time` configuration is applied to all members of `interface-range range-1`.

This can be verified with `show interfaces | display inheritance` as follows:

```
user@host# show interfaces | display inheritance
ge-1/0/0 {
    ## '256' was expanded from interface-range 'range-1'
    ## mtu 256;
    ## 'hold-time' was inherited from group 'global'
    ## '10' was inherited from group 'global'
    ## hold-time up 10;
}
ge-1/0/1 {
    ##
    ## '256' was expanded from interface-range 'range-1'
```
See Also • Using Wildcards with Configuration Groups

Interfaces Inheriting Common Configuration

If an interface is a member of several interface ranges, that interface will inherit the common configuration from all of those interface ranges.

```
[edit]
interfaces {
    interface-range range-1 {
        member-range ge-1/0/0 to ge-10/0/47;
        mtu 256;
    }
}
```

In this example, interfaces ge-10/0/0 through ge-10/0/47 will have both hold-time and mtu.

Configuring Inheritance Range Priorities

The interface ranges are defined in the order of inheritance priority, with the first interface range configuration data taking priority over subsequent interface ranges.

```
[edit]
interfaces {
    interface-range int-grp-one {
        member-range ge-0/0/0 to ge-4/0/40;
        member ge-1/1/1;
    }
}
/*Common config is added part of the interface-range definition*/
mtu 256;
hold-time up 10;
}
}
} interfaces {
interface-range int-grp-two {
   member-range ge-5/0/0 to ge-10/0/40;
   member ge-1/1/1;
   mtu 1024;
}
}
}
}

Interface ge-1/1/1 exists in both interface-range int-grp-one and interface-range int-grp-two. This interface inherits mtu 256 from interface-range int-grp-one because it was defined first.

Configuration Expansion Where Interface Range Is Used

In this example, interface-range range-1 is used under the protocols hierarchy:

[edit]
interfaces {
   interface-range range-1 {
      member ge-10/1/1;
      member ge-5/5/1;
      mtu 256;
      hold-time up 10;
      ether-options {
         flow-control;
         speed {
            100m;
         }
         802.3ad primary;
      }
   }
   protocols {
      dot1x {
         authenticator {
            interface range-1 {
               retries 1;
            }
         }
      }
   }
}

The interface node present under authenticator is expanded into member interfaces of the interface-range range-1 as follows:

protocols {
   dot1x {
      authenticator {
         interface ge-10/1/1 {

The `interface range` statement is expanded into two interfaces, `ge-10/1/1` and `ge-5/5/1`, and configuration `retries 1` is copied under those two interfaces.

This configuration can be verified using the `show protocols dot1x | display inheritance` command.

**Related Documentation**
- Physical Interfaces

### Specifying an Aggregated Interface

The M Series, MX Series, and T Series routers support aggregated interfaces. To specify an aggregated interface assign a number with the aggregated interface name. For example, configure `aex` at the `[edit interfaces]` hierarchy level, where `x` is an integer ranging 0 through 127 for M Series and T Series routers and 0 through 479 on MX Series routers.

For aggregated SONET/SDH interfaces, configure `asx` at the `[edit interfaces]` hierarchy level.

**NOTE:** SONET/SDH aggregation is proprietary to the Junos OS and might not work with other software.

If you are configuring VLANs for aggregated Ethernet interfaces, you must include the `vlan-tagging` statement at the `[edit interfaces aex]` hierarchy level to complete the association.

**Related Documentation**
- Aggregated Ethernet Interfaces Overview
- Configuring Aggregated SONET/SDH Interfaces

### Media MTU Overview

The media maximum transmission unit (MTU) is the largest data unit that can be forwarded without fragmentation.

The default media MTU size used on a physical interface depends on the encapsulation used on that interface. In some cases, the default IP Protocol MTU depends on whether the protocol used is IP version 4 (IPv4) or International Organization for Standardization (ISO).
The default media MTU is calculated as follows:

\[
\text{Default media MTU} = \text{Default IP MTU} + \text{encapsulation overhead}
\]

When you are configuring point-to-point connections, the MTU sizes on both sides of the connections must be the same. Also, when you are configuring point-to-multipoint connections, all interfaces in the subnet must use the same MTU size.

NOTE: The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the media MTU. For example, the media MTU for a Gigabit Ethernet Version 2 interface is specified as 1514 bytes, but the largest possible frame size is actually 1518 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.

The physical MTU for Ethernet interfaces does not include the 4-byte frame check sequence (FCS) field of the Ethernet frame.

A SONET/SDH interface operating in concatenated mode has a “c” added to the rate descriptor. For example, a concatenated OC48 interface is referred to as OC48c.

If you do not configure an MPLS MTU, the Junos OS derives the MPLS MTU from the physical interface MTU. From this value, the software subtracts the encapsulation-specific overhead and space for the maximum number of labels that might be pushed in the Packet Forwarding Engine. Currently, the software provides for three labels of four bytes each, for a total of 12 bytes.

In other words, the formula used to determine the MPLS MTU is the following:

\[
\text{MPLS MTU} = \text{physical interface MTU} - \text{encapsulation overhead} - 12
\]

Media MTU Sizes by Interface Type

The media maximum transmission unit (MTU) is the largest data unit that can be forwarded without fragmentation.

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead.
This topic includes following information:

- Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers on page 86
- Media MTU Sizes by Interface Type for M40e Routers on page 87
- Media MTU Sizes by Interface Type for M160 Routers on page 88
- Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers on page 89
- Media MTU Sizes by Interface Type for MX Series Routers on page 90
- Media MTU Sizes by Interface Type for T320 Routers on page 91
- Media MTU Sizes by Interface Type for T640 Platforms on page 92
- Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers on page 92
- Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers on page 93

### Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers

Table 9: Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services (MTU size not configurable)</td>
<td>9192</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ATM</td>
<td>4470</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (8-port)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (12-port)</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> The maximum MTU for two 100Base-TX Fast Ethernet port FIC is 9192 bytes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The maximum MTU for one Gigabit Ethernet port FIC is 9192 bytes.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 9: Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for M40e Routers

### Table 10: Media MTU Sizes by Interface Type for M40e Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services</td>
<td>9192</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>E3/DS3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192 (1- or 2-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port)</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
</tbody>
</table>
### Table 10: Media MTU Sizes by Interface Type for M40e Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>4500 (1-port nonconcatenated)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port OC3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port OC3c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC12)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port OC12)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port OC12c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC48)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (2-port OC3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (2-port OC3c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC12c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC48c)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC192)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC192c)</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for M160 Routers

### Table 11: Media MTU Sizes by Interface Type for M160 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services</td>
<td>9192</td>
<td>N/A</td>
</tr>
<tr>
<td>(MTU size not configurable)</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
</tr>
<tr>
<td>4470</td>
<td></td>
<td>AT-M</td>
</tr>
<tr>
<td>1500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>4500</td>
</tr>
<tr>
<td>1500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>4500</td>
</tr>
<tr>
<td>4470</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E3/DS3 I/Q</td>
<td>4474</td>
<td>9192</td>
</tr>
<tr>
<td>4470</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533</td>
</tr>
<tr>
<td>1500 (IPv4), 1497 (ISO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192 (1- or 2-port)</td>
</tr>
<tr>
<td>1500 (IPv4), 1497 (ISO)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 11: Media MTU Sizes by Interface Type for M160 Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>4500 (1-port nonconcatenated)</td>
<td>4470</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1- or 2-port)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port)</td>
<td></td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers

### Table 12: Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM2 IQ</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized DS3 IQ</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized E1 IQ</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>Channelized OC12 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized STM1 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>DS3</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>E1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3 IQ</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (8-, 12- and 48-port)</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
</tbody>
</table>
### Table 12: Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT3 IQ (excluding M120)</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for MX Series Routers

**Table 13: Media MTU Sizes by Interface Type for MX Series Routers**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>• 9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>• 9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>Multi-Rate Ethernet</td>
<td>1514</td>
<td>• 9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>Tri-Rate Ethernet</td>
<td>1514</td>
<td>• 9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>Channelized SONET/SDH OC3/STM1 (Multi-Rate)</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>DS3/E3 (Multi-Rate)</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
</tbody>
</table>

**NOTE:** Starting in Junos OS Release 16.1R1, the MTU size for a media or protocol is increased from 9192 to 9500 for Ethernet interfaces on the following MX Series MPCs:

- MPC1
- MPC2
- MPC2E
- MPC3E
- MPC4E
- MPC5E
- MPC6E
NOTE: Starting in Junos OS Release 16.1R1, the MTU size for a media or protocol is increased from 9192 to 9500 for Ethernet interfaces on the following MX Series MPCs:

- MPC1
- MPC2
- MPC2E
- MPC3E
- MPC4E
- MPC5E
- MPC6E

Starting in Junos OS Release 16.1R1, the MTU size has been increased to 16,000 bytes for certain MPCs. The MTU size for the following MPCs has been increased to 16000 bytes:

- MPC7E (MPC7E-MRATE and MP7E-10G)
- MPC8E (MX2K-MPC8E)
- MPC9E (MX2K-MPC9E)

Starting in Junos OS Release 17.3R1, the MTU size for MX10003 MPC is 16,000 bytes.

Starting in Junos OS Release 17.4R1, the MTU size for MX204 is 16,000 bytes.

In all Junos OS releases, the maximum MTU size for MX5, MX10, MX40, and MX80 routers is 9192 bytes.

In all Junos OS releases, the maximum MTU size for MPC2E-NG and MPC3E-NG is 9500 bytes.

**Media MTU Sizes by Interface Type for T320 Routers**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4470</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>ATM2 IQ</td>
<td>4472</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized OC12 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized STM1 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>DS3</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
</tbody>
</table>
### Table 14: Media MTU Sizes by Interface Type for T320 Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (12- and 48-port)</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>CT3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for T640 Platforms

### Table 15: Media MTU Sizes by Interface Type for T640 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM2 IQ</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>48-port Fast Ethernet</td>
<td>1514</td>
<td>1532</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>CT3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers

### Table 16: Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
</tbody>
</table>
NOTE: On ACX Series routers, you can configure the protocol MTU by including the mtu statement at the [edit interfaces interface-name unit logical-unit-number family inet] or [edit interfaces interface-name unit logical-unit-number family inet6] hierarchy level.

- If you configure the protocol MTU at any of these hierarchy levels, the configured value is applied to all families that are configured on the logical interface.
- If you are configuring the protocol MTU for both inet and inet6 families on the same logical interface, you must configure the same value for both the families. It is not recommended to configure different MTU size values for inet and inet6 families that are configured on the same logical interface.

### Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers

**Table 17: Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>40-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>100-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
</tbody>
</table>

### 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, the MTU size for MX204 is 16,000 bytes.</td>
</tr>
<tr>
<td>17.3R1</td>
<td>Starting in Junos OS Release 17.3R1, the MTU size for MX10003 MPC is 16,000 bytes.</td>
</tr>
<tr>
<td>16.1R1</td>
<td>Starting in Junos OS Release 16.1R1, the MTU size has been increased to 16,000 bytes for certain MPCs.</td>
</tr>
</tbody>
</table>

### Related Documentation
- Encapsulation Overhead by Interface Encapsulation Type on page 97
- Configuring the Media MTU on page 99
- Media MTU Overview on page 84
Media MTU Overview

The default media MTU size used on a physical interface depends on the encapsulation used on that interface. In some cases, the default IP Protocol MTU depends on whether the protocol used is IP version 4 (IPv4) or International Organization for Standardization (ISO).

The default media MTU is calculated as follows:

\[
\text{Default media MTU} = \text{Default IP MTU} + \text{encapsulation overhead}
\]

When you are configuring point-to-point connections, the MTU sizes on both sides of the connections must be the same. Also, when you are configuring point-to-multipoint connections, all interfaces in the subnet must use the same MTU size. For details about encapsulation overhead, see “Encapsulation Overhead by Encapsulation Type” on page 95.

NOTE: The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the media MTU. For example, the media MTU for a Gigabit Ethernet Version 2 interface is specified as 1514 bytes, but the largest possible frame size is actually 1518 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.

The physical MTU for Ethernet interfaces does not include the 4-byte frame check sequence (FCS) field of the Ethernet frame.

If you do not configure an MPLS MTU, the Junos OS derives the MPLS MTU from the physical interface MTU. From this value, the software subtracts the encapsulation-specific overhead and space for the maximum number of labels that might be pushed in the Packet Forwarding Engine. Currently, the software provides for three labels of four bytes each, for a total of 12 bytes.

In other words, the formula used to determine the MPLS MTU is the following:

\[
\text{MPLS MTU} = \text{physical interface MTU} - \text{encapsulation overhead} - 12
\]

If you configure an MTU value by including the mtu statement at the [edit interfaces interface-name unit logical-unit-number family mpls] hierarchy level, the configured value is used. Junos OS Release 16.2R1.6 and later releases do not support family mpls MTU.
How to Configure the Media MTU

To modify the default media MTU size for a physical interface, include the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead.

**NOTE:** Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

You configure the protocol MTU by including the `mtu` statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family inet]`
- `[edit interfaces interface-name unit logical-unit-number family inet6]`

If you configure the protocol MTU at any of these hierarchy levels, the configured value is applied to all families that are configured on the logical interface.

**NOTE:** If you are configuring the protocol MTU for both inet and inet6 families on the same logical interface, you must configure the same value for both the families. It is not recommended to configure different MTU size values for inet and inet6 families that are configured on the same logical interface.

Encapsulation Overhead by Encapsulation Type

**Table 18: Encapsulation Overhead by Encapsulation Type**

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q/Ethernet 802.3</td>
<td>21</td>
</tr>
<tr>
<td>802.1Q/Ethernet Subnetwork Access Protocol (SNAP)</td>
<td>26</td>
</tr>
<tr>
<td>802.1Q/Ethernet version 2</td>
<td>18</td>
</tr>
<tr>
<td>ATM Cell Relay</td>
<td>4</td>
</tr>
<tr>
<td>ATM permanent virtual connection (PVC)</td>
<td>12</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet 802.3</td>
<td>17</td>
</tr>
</tbody>
</table>
### Table 18: Encapsulation Overhead by Encapsulation Type (continued)

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet circuit cross-connect (CCC) and virtual private LAN service (VPLS)</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet over ATM</td>
<td>32</td>
</tr>
<tr>
<td>Ethernet SNAP</td>
<td>22</td>
</tr>
<tr>
<td>Ethernet translational cross-connect (TCC)</td>
<td>18</td>
</tr>
<tr>
<td>Ethernet version 2</td>
<td>14</td>
</tr>
<tr>
<td>Extended virtual local area network (VLAN) CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Extended VLAN TCC</td>
<td>22</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>4</td>
</tr>
<tr>
<td>PPP</td>
<td>4</td>
</tr>
<tr>
<td>VLAN CCC</td>
<td>4</td>
</tr>
<tr>
<td>VLAN VPLS</td>
<td>4</td>
</tr>
<tr>
<td>VLAN TCC</td>
<td>22</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for ACX Series Routers

#### Table 19: Media MTU Sizes by Interface Type for ACX Series Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
</tbody>
</table>

### Related Documentation
- Configuring Interface Encapsulation on Physical Interfaces on page 114
- Setting the Protocol MTU on page 209
Encapsulation Overhead by Interface Encapsulation Type

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. The following table lists the interface encapsulation and corresponding encapsulation overhead.

Table 20: Encapsulation Overhead by Encapsulation Type

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q/Ethernet 802.3</td>
<td>21</td>
</tr>
<tr>
<td>802.1Q/Ethernet Subnetwork Access Protocol (SNAP)</td>
<td>26</td>
</tr>
<tr>
<td>802.1Q/Ethernet version 2</td>
<td>18</td>
</tr>
<tr>
<td>ATM Cell Relay</td>
<td>4</td>
</tr>
<tr>
<td>ATM permanent virtual connection (PVC)</td>
<td>12</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet 802.3</td>
<td>17</td>
</tr>
<tr>
<td>Ethernet circuit cross-connect (CCC) and virtual private LAN service (VPLS)</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet over ATM</td>
<td>32</td>
</tr>
<tr>
<td>Ethernet SNAP</td>
<td>22</td>
</tr>
<tr>
<td>Ethernet translational cross-connect (TCC)</td>
<td>18</td>
</tr>
<tr>
<td>Ethernet version 2</td>
<td>14</td>
</tr>
<tr>
<td>Extended virtual local area network (VLAN) CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Extended VLAN TCC</td>
<td>22</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>4</td>
</tr>
<tr>
<td>PPP</td>
<td>4</td>
</tr>
<tr>
<td>VLAN CCC</td>
<td>4</td>
</tr>
<tr>
<td>VLAN VPLS</td>
<td>4</td>
</tr>
<tr>
<td>VLAN TCC</td>
<td>22</td>
</tr>
</tbody>
</table>
Configuring Interface Description

You can include a text description of each physical interface in the configuration file. Any descriptive text you include is displayed in the output of the `show interfaces` commands, and is also exposed in the `ifAlias` Management Information Base (MIB) object. It has no impact on the interface's configuration.

To add a text description, include the `description` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit]
user@host# set interfaces interface-name description text
```

For example:

```
[edit]
user@host# set interfaces fe-0/0/1 description "Backbone connection to PHL01"
```

The description can be a single line of text. If the text contains spaces, enclose it in quotation marks.

---

**NOTE:** You can configure the extended DHCP relay to include the interface description in the option 82 Agent Circuit ID suboption. See *Using DHCP Relay Agent Option 82 Information* in the *Junos OS Broadband Subscriber Management and Services Library*.

---

For information about describing logical units, see “Adding a Logical Unit Description to the Configuration” on page 172.

To display the description from the router or switch CLI, use the `show interfaces` command:

```
user@host> show interfaces fe-0/0/1
Physical interface: fe-0/0/1, Enabled, Physical link is Up
   Interface index: 129, SNMP ifIndex: 23
   Description: Backbone connection to PHL01
```

To display the interface description from the interfaces MIB, use the `snmpwalk` command from a server. To isolate information for a specific interface, search for the interface index.
shown in the **SNMP ifIndex** field of the **show interfaces** command output. The **ifAlias** object is in IFXTable.

```plaintext
user-server> snmpwalk host-fxp0.mylab public ifXTable | grep -e '\.23'

```

```plaintext
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.23 = fe-0/0/1
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifInMulticastPkts.23 = Counter32: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifInBroadcastPkts.23 = Counter32: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifOutMulticastPkts.23 = Counter32: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifOutBroadcastPkts.23 = Counter32: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInUcastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInMulticastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInBroadcastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutOctets.23 = Counter64: 42
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutUcastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutMulticastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutBroadcastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCInOctets.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutOctets.23 = Counter64: 100
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutMulticastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutBroadcastPkts.23 = Counter64: 0
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifLinkUpDownTrapEnable.23 = enabled(1)
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHighSpeed.23 = Gauge32: 100
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifPromiscuousMode.23 = false(2)
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifConnectorPresent.23 = true(1)
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifAlias.23 = Backbone connection to PHL01
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifCounterDiscontinuityTime.23 = Timeticks: (0) 0:00:00.00
```

### Related Documentation

- [Using DHCP Relay Agent Option 82 Information](#)
- [Adding a Logical Unit Description to the Configuration on page 172](#)

## Configuring the Media MTU

The media maximum transmission unit (MTU) is the largest data unit that can be forwarded without fragmentation. The default media MTU size used on a physical interface depends on the encapsulation being used on that interface. For a listing of MTU sizes for each encapsulation type, see “Media MTU Sizes by Interface Type” on page 85.

To configure the media-MTU size:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   ```plaintext
   [edit ]
   user@host# [edit interfaces interface-name]
   ```

2. Include the `mtu` statement.

   ```plaintext
   [edit interfaces interface-name]
   mtu bytes;
   ```

   - If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. You
configure the protocol MTU by including the `mtu` statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

**NOTE:**
- Changing the media MTU or protocol MTU causes an interface to be deleted and added again.
- Because tunnel services interfaces are considered logical interfaces, you cannot configure the MTU setting for the physical interface. This means you cannot include the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level for the following interface types: generic routing encapsulation (gr-), IP-IP (ip-), loopback (lo-), link services (ls-), multilink services (ml-), and multicast (pe-, pd-). You can, however, configure the protocol MTU on all tunnel interfaces except virtual tunnel (vt) interfaces. Starting in Junos OS Release 17.1R3, you cannot configure the maximum transmission unit (MTU) size for vt interfaces because the `mtu bytes` option is deprecated for vt interfaces. Junos OS sets the MTU size for vt interfaces by default to unlimited.
- If you configure an MTU value by including the `mtu` statement at the `[edit interfaces interface-name unit logical-unit-number family mpls]` hierarchy level, the configured value is used.

**Related Documentation**
- Media MTU Overview on page 84
- Media MTU Sizes by Interface Type on page 85
- Encapsulation Overhead by Interface Encapsulation Type on page 97

**Configuring the Interface Speed**

You can configure the interface speed in following ways:

- Configuring the Interface Speed on Ethernet Interfaces on page 100
- Configuring Aggregated Ethernet Link Speed on page 102
- Configuring SONET/SDH Interface Speed on page 104

**Configuring the Interface Speed on Ethernet Interfaces**

For M Series and T Series Fast Ethernet 12-port and 48-port PIC interfaces, the management Ethernet interface (`fxp0` or `em0`), and the MX Series Tri-Rate Ethernet copper interfaces, you can explicitly set the interface speed. The Fast Ethernet, `fxp0`, and `em0` interfaces can be configured for 10 Mbps or 100 Mbps (`10m` | `100m`). The MX Series Tri-Rate Ethernet copper interfaces can be configured for 10 Mbps, 100 Mbps, or 1 Gbps.
(10m | 100m | 1g). For information about management Ethernet interfaces and to
determine the management Ethernet interface type for your router, see “Understanding
Management Ethernet Interfaces” on page 10 and Supported Routing Engines by RouterMX
Series routers, with MX-DPC and Tri-Rate Copper SFPs, support 20x1 Copper to provide
backwards compatibility with 100/10BASE-T and 1000BASE-T operation through an
Serial Gigabit Media Independent Interface (SGMII) interface.

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level.

   [edit ]
   user@host# edit interfaces interface-name

2. To configure the speed, include the speed statement at the [edit interfaces
   interface-name] hierarchy level.

   [edit interfaces interface-name]
   user@host# set speed (10m | 100m | 1g | auto | auto-10m-100m);
NOTE:

- By default, the M Series and T Series routers management Ethernet interface autonegotiates whether to operate at 10 megabits per second (Mbps) or 100 Mbps. All other interfaces automatically choose the correct speed based on the PIC type and whether the PIC is configured to operate in multiplexed mode (using the no-concatenate statement in the [edit chassis] configuration hierarchy.

- Starting with Junos OS Release 14.2 the auto-10m-100m option allows the fixed tri-speed port to auto negotiate with ports limited by 100m or 10m maximum speed. This option must be enabled only for Tri-rate MPC port, that is, 3D 40x 1GE (LAN) RJ45 MIC on MX platform. This option does not support other MICs on MX platform.

- When you manually configure Fast Ethernet interfaces on the M Series and T Series routers, link mode and speed must both be configured. If both these values are not configured, the router uses autonegotiation for the link and ignores the user-configured settings.

- If the link partner does not support autonegotiation, configure either Fast Ethernet port manually to match its link partner's speed and link mode. When the link mode is configured, autonegotiation is disabled.

- On MX Series routers with tri-rate copper SFP interfaces, if the port speed is negotiated to the configured value and the negotiated speed and interface speed do not match, the link will not be brought up.

- When you configure the Tri-Rate Ethernet copper interface to operate at 1Gbps, autonegotiation must be enabled.

- Starting with Junos OS Release 11.4, half-duplex mode is not supported on Tri-Rate Ethernet copper interfaces. When you include the speed statement, you must include the link-mode full-duplex statement at the same hierarchy level.

See Also  speed on page 1008

Configuring Aggregated Ethernet Link Speed

On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. Generally, all interfaces that make up a bundle must have the same speed. If you include in the aggregated Ethernet interface an individual link that has a speed different from the speed that you specify in the link-speed parameter, an error message is logged. However, there are exceptions.

Starting with Junos OS Release 13.2, aggregated Ethernet supports mixed rates and mixed modes on T640, T1600, T4000, and TX Matrix Plus routers. For example, these mixes are supported:

- Member links of different modes (WAN and LAN) for 10-Gigabit Ethernet links.
• Member links of different rates: 10-Gigabit Ethernet, 40-Gigabit Ethernet, 50-Gigabit Ethernet, 100-Gigabit Ethernet, and OC192 (10-Gigabit Ethernet WAN mode)

Starting with Junos OS Release 14.1R1 and 14.2, support for mixed rates on aggregated Ethernet bundles is extended to MX240, MX480, MX960, MX2010, and MX2020 routers.

Starting with Junos OS Release 14.2, aggregated Ethernet supports mixed link speeds on PTX Series Packet Transport Routers.

NOTE:
• Member links of 50-Gigabit Ethernet can only be configured using the 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP (PD-ICE-CFP-FPC4).

• Starting with Junos OS Release 13.2, 100-Gigabit Ethernet member links can be configured using the two 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP. This 100-Gigabit Ethernet member link can be included in an aggregated Ethernet link that includes member links of other interfaces as well. In releases before Junos OS Release 13.2, the 100-Gigabit Ethernet member link configured using the two 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP cannot be included in an aggregated Ethernet link that includes member links of other interfaces.

To configure member links of mixed rates and mixed modes on T640, T1600, T4000, TX Matrix Plus, and PTX routers, you need to configure the mixed option for the [edit interfaces aex aggregated-ether-options link-speed] statement.

To set the required link speed:

1. Specify that you want to configure the aggregated Ethernet options.

   user@host# edit interfaces interface-name aggregated-ether-options

2. Configure the link speed.

   [edit interfaces interface-name aggregated-ether-options ]
   user@host# set link-speed speed

   speed can be in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

   Aggregated Ethernet interfaces on the M120 router can have one of the following speeds:

   • 100m—Links are 100 Mbps.
   • 10g—Links are 10 Gbps.
• 1g—Links are 1 Gbps.
• oc192—Links are OC192 or STM64c.

Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speeds:

• 10m—Links are 10 Mbps.
• 100m—Links are 100 Mbps.
• 1g—Links are 1 Gbps.
• 10g—Links are 10 Gbps.
• 50g—Links are 50 Gbps.

Aggregated Ethernet links on T Series, MX Series, PTX Series routers, and QFX5100, QFX10002, QFX10008, and QFX10016 switches can be configured to operate at one of the following speeds:

• 100g—Links are 100 Gbps.
• 100m—Links are 100 Mbps.
• 10g—Links are 10 Gbps.
• 1g—Links are 1 Gbps.
• 40g—Links are 40 Gbps.
• 50g—Links are 50 Gbps.
• 80g—Links are 80 Gbps.
• 8g—Links are 8 Gbps.
• mixed—Links are of various speeds.
• oc192—Links are OC192.

See Also  • aggregated-ether-options on page 415

Configuring SONET/SDH Interface Speed

To configure the speed of SONET/SDH interfaces in concatenated mode:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level, where the interface-name is so-fpc/pic/port.

   [edit]
   user@host# edit interfaces so-fpc/pic/port

2. Configure interface speed in concatenated mode.

   For example, each port of 4-port OC12 PIC can be configured to be in OC3 or OC12 speed independently when this PIC is in 4xOC12 concatenated mode.
To configure the speed of SONET/SDH interfaces in nonconcatenated mode:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level, where the `interface-name` is `so-fpc/pic/port`.

   ```
   [edit]
   user@host# edit interfaces so-fpc/pic/port
   ```

2. Configure interface speed in nonconcatenated mode.
   For example, each port of 4-port OC12 PIC can be configured to be in OC3 or OC12 speed independently when this PIC is in 4xOC12 concatenated mode.

   ```
   [edit interfaces so-fpc/pic/port]
   user@host# set speed (oc3 | oc12 | oc48)
   ```

To configure the PIC to operate in channelized (multiplexed) mode:

1. In configuration mode, go to the `[edit chassis fpc slot-number pic pic-number]` hierarchy level.

   ```
   [edit]
   user@host# [edit chassis fpc slot-number pic pic-number]
   ```

2. Configure the `no-concatenate` option.

   ```
   [edit interfaces so-fpc/pic/port]
   user@host# set no-concatenate
   ```

**NOTE:** On SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP, you cannot set the interface speed at the `[edit interfaces]` hierarchy level. To enable the speed on these MICs, you need to set the port speed at the `[edit chassis fpc slot-number pic pic-number port port-number]` hierarchy level.

For more information about using the non-concatenate statement, see the Junos OS Administration Library.

**See Also**
- Configuring SONET/SDH Physical Interface Properties
- SONET/SDH Interface Speed Overview
SONET/SDH Interfaces Overview

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 auto-10m-100m option allows the fixed tri-speed port to auto-negotiate with ports limited by 100m or 10m maximum speed. This option must be enabled only for Tri-rate MPC port, that is, 3D 40x 1GE (LAN) RJ45 MIC on MX platform. This option does not support other MICs on MX platform.</td>
</tr>
<tr>
<td>14.2</td>
<td>Starting with Junos OS Release 14.2, aggregated Ethernet supports mixed link speeds on PTX Series Packet Transport Routers.</td>
</tr>
<tr>
<td>14.1</td>
<td>Starting with Junos OS Release 14.1R1 and 14.2, support for mixed rates on aggregated Ethernet bundles is extended to MX240, MX480, MX960, MX2010, and MX2020 routers.</td>
</tr>
<tr>
<td>13.2</td>
<td>Starting with Junos OS Release 13.2, aggregated Ethernet supports mixed rates and mixed modes on T640, T1600, T4000, and TX Matrix Plus routers.</td>
</tr>
<tr>
<td>13.2</td>
<td>Starting with Junos OS Release 13.2, 100-Gigabit Ethernet member links can be configured using the two 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP.</td>
</tr>
<tr>
<td>11.4</td>
<td>Starting with Junos OS Release 11.4, half-duplex mode is not supported on Tri-Rate Ethernet copper interfaces. When you include the speed statement, you must include the link-mode full-duplex statement at the same hierarchy level.</td>
</tr>
</tbody>
</table>

Related Documentation

Configuring the Link Characteristics

By default, the router’s management Ethernet interface, fxp0 or em0, autonegotiates whether to operate in full-duplex or half-duplex mode. Fast Ethernet interfaces can operate in either full-duplex or half-duplex mode, and all other interfaces can operate only in full-duplex mode. For Gigabit Ethernet, the link partner must also be set to full duplex.

---

**NOTE:** When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled.

---

**NOTE:** When you manually configure Fast Ethernet interfaces on the M Series and T Series routers, link mode and speed must both be configured. If both these values are not configured, the router uses autonegotiation for the link and ignores the user-configured settings.
NOTE: When the Fast Ethernet interface on Juniper Networks routers with autonegotiation enabled interoperates with a device configured to operate in half-duplex mode (autonegotiation disabled), the interface defaults to half-duplex mode after the PIC is taken offline and brought back online. This results in packet loss and cyclic redundancy check (CRC) errors.

To explicitly configure an Ethernet interface to operate in either full-duplex or half-duplex mode, include the link-mode statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
link-mode (full-duplex | half-duplex);
```

### Interface Alias Names Overview

You can configure a textual description of a logical unit on a physical interface to be the alias of an interface name. Interface aliasing is supported only at the unit level. If you configure an alias name, the alias name is displayed instead of the interface name in the output of all show, show interfaces, and other operational mode commands. In Junos OS Release 12.3R8 and later, display of the alias can be suppressed in favor of the actual interface name by using the display no-interface-alias parameter along with the show command. Configuring an alias for a logical unit of an interface has no effect on how the interface on the router or switch operates.

When you configure the alias name of an interface, the CLI saves the alias name as the value of the interface-name variable in the configuration database. To enable backward compatibility with Junos OS releases in which the support for interface aliases is not available, when the Junos OS processes query the configuration database for the interface-name variable, the actual, exact value of the interface-name variable is returned instead of the alias name for system operations and computations.

This capability to define interface alias names for physical and logical interfaces is useful in a Junos Node Unifier (JNU) environment that contains a Juniper Networks MX Series 5G Universal Routing Platform as a controller and EX Series Ethernet switches, QFX Series devices, and ACX Series Universal Metro Routers as satellite devices. The following are the benefits of configuring an alias name, which enables a meaningful, single, and easily identifiable name to be allocated to an interface:

- You can group physical interfaces as one aggregated interface (link aggregation group or LAG bundle) and name that bundle as a satellite connection interface (for example, sat1).
- You can select a logical interface as a member of the LAG bundle or the entire LAG, and name that interface to represent a satellite device port or a service instance (for example, ge-0/0/1).
- You can combine the satellite name and the interface name aliases to wholly represent the satellite port name (for example, sat1:ge-0/0/1 or ge-sat1/0/0/1 or ge-1/0/0/1)
the most easily distinguishable format that denotes a combination of port and satellite parts of the name.

To specify an interface alias, you can use the alias statement at the [edit interfaces interface-name unit logical-unit-number] and [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number] hierarchy levels.

NOTE: In Juniper Networks M Series Multiservice Edge Routers, if the same alias name is configured on more than one logical interface, the router displays an error message and commit fails.

Example: Adding an Interface Alias Name

This example shows how to add an alias to the logical unit of an interface. Using an alias to identify interfaces as they appear in the output for operational commands can allow for more meaningful naming conventions and easier identification.

- Requirements on page 108
- Overview on page 108
- Configuration on page 108
- Verification on page 111

Requirements

This example uses the following hardware and software components:

- One MX Series router that acts as a controller
- One EX4200 switch that acts as a satellite device
- Junos OS Release 13.3R1 or later

Overview

You can create an alias for each logical unit on a physical interface. The descriptive text you define for the alias is displayed in the output of the show interfaces commands. In Junos OS Release 12.3R8 and later, display of the alias can be suppressed in favor of the actual interface name by using the display no-interface-alias parameter along with the show command. The alias configured for a logical unit of an interface has no effect on how the interface on the router or switch operates — it is only a cosmetic label.

Configuration

Consider a scenario in which alias names are configured on the interfaces of a JNU controller that are connected to a satellite, sat1, in the downlink direction in the JNU
management network by using two links. The alias names enable effective, streamlined identification of these interfaces in the operational mode commands that are run on the controller and satellites.

- Configuring Alias Names for the Controller Interfaces on page 109
- Results on page 110

### 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 commands into the CLI at the [edit] hierarchy level:

```
set interfaces ae0 unit 0 alias "controller-sat1-downlink1"
set interfaces ae0.0 family inet address 10.0.0.1/24
set interfaces ae1 unit 0 alias "controller-sat1-downlink1"
set interfaces ae0.0 family inet address 192.0.2.128/25
set interfaces ge-0/0/0 vlan-tagging
set interfaces ge-0/0/0 unit 0 alias "ge-to-corp-gw1"
set interfaces ge-0/0/0.0 vlan-id 101
set interfaces ge-0/1/0 gigether-options 802.3adae0
set interfaces ge-0/1/1 gigether-options 802.3adae0
set protocols rip group corporate-firewall neighbor ge-to-corp-gw1
```

### Configuring Alias Names for the Controller Interfaces

#### 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 in the CLI User Guide.

To add an alias name to the controller interfaces that are used to connect to the satellite devices in the downlink direction:

1. Configure an alias name for the logical unit of an aggregated Ethernet interface that is used to connect to a satellite, sat1, in the downlink direction. Configure inet family and address for the interface.

   ```
   [edit]
   user@host# set interfaces ae0 unit 0 alias "controller-sat1-downlink1"
   user@host# set interfaces ae0.0 family inet address 10.0.0.1/24
   ```

2. Configure an alias name for the logical unit of another aggregated Ethernet interface that is used to connect to the same satellite, sat1, in downlink direction. Configure INET family and address for the interface.

   ```
   [edit]
   user@host# set interfaces ae0 unit 1 alias "controller-sat1-downlink2"
   user@host# set interfaces ae0.0 family inet address 10.0.0.3/24
   ```
3. Configure an alias name for the Gigabit Ethernet interface on the controller and configure its parameters.

```
[edit]
user@host# set interfaces ge-0/0/0 vlan-tagging
user@host# set interfaces ge-0/0/0 unit 0 alias "ge-to-corp-gw1"
user@host# set interfaces ge-0/0/0/0 vlan-id 101
user@host# set interfaces ge-0/0/0/0 family inet address 1.1.1.1/23
```

4. Configure Gigabit Ethernet interfaces to be member links of an ae- logical interface.

```
[edit]
user@host# set interfaces ge-0/1/0 gigether-options 802.3ad ae0
user@host# set interfaces ge-0/1/1 gigether-options 802.3ad ae0
```

5. Configure RIP in the network between the controller and the firewall gateway.

```
[edit]
user@host# set protocols rip group corporate-firewall neighbor ge-to-corp-gw1
```

**Results**

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

```
[edit]
interfaces {
    ae0 {
        unit 0 {
            alias "controller-sat1-downlink1";
            family inet {
                address 10.0.0.1/24;
            }
        }
        unit 1 {
            alias "controller-sat1-downlink2";
            family inet {
                address 10.0.0.3/24;
            }
        }
    }
    ge-0/0/0 {
        vlan-tagging;
        unit 0 {
            alias "ge-to-corp-gw1";
            vlan-id 101;
            family inet {
                address 1.1.1.1/23;
            }
        }
    }
}
```
After you have confirmed that the interfaces are configured, enter the **commit** command in configuration mode.

**NOTE:** In Juniper Networks M Series Multiservice Edge Routers, if the same alias name is configured on more than one logical interface, the router displays an error message and commit fails.

### Verification

To verify that the alias name is displayed instead of the interface name, perform these steps:

1. Verifying the Configuration of the Alias Name for the Controller Interfaces on page 111

#### Verifying the Configuration of the Alias Name for the Controller Interfaces

**Purpose**

Verify that the alias name is displayed instead of the interface name.

**Action**

Display information about all RIP neighbors.

```
user@router> show rip neighbor
```

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Local State</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Send Mode</th>
<th>Receive Mode</th>
<th>In Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-to-corp-gw1</td>
<td>DN (null)</td>
<td>255.255.255.255 mcast</td>
<td>both</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**

The output displays the details of the benchmarking test that was performed. For more information about the **show rip neighbor** operational command, see **show rip neighbor** in the CLI Explorer.
Clock Source Overview

For both the router and interfaces, the clock source can be an external clock that is received on the interface or the router’s internal Stratum 3 clock.

For example, interface A can transmit on interface A’s received clock (external, loop timing) or the Stratum 3 clock (internal, line timing, or normal timing). Interface A cannot use a clock from any other source. For interfaces such as SONET/SDH that can use different clock sources, you can configure the source of the transmit clock on each interface.

The clock source resides on the System Control Board (SCB) for M40 routers, the System and Switch Board (SSB) for M20 routers, the Control Board (CB) for M120 routers, and the Miscellaneous Control Subsystem (MCS) for M40e and M160 routers. M7i and M10i routers have a clock source on the Compact Forwarding Engine Board (CFEB) and Enhanced Compact Forwarding Engine Board (CFEB-E).

For T Series and MX Series, the clock source internal Stratum 3 clock resides on the SONET Clock Generator and Switch Control Board (SCB) respectively. By default, the 19.44-MHz Stratum 3 reference clock generates the clock signal for all serial PICs (SONET/SDH) and Plesiochronous Digital Hierarchy (PDH) PICs. PDH PICs include DS3, E3, T1, and E1 PICs.

NOTE: M7i and M10i routers do not support external clocking of SONET interfaces.

For information about clocking on channelized interfaces, see Channelized IQ and IQE Interfaces Properties. Also see Configuring the Clock Source on SONET/SDH Interfaces and Configuring the Channelized T3 Loop Timing.

For information about configuring an external synchronization interface that can be used to synchronize the internal Stratum 3 clock to an external source on the M40e, M120, M320, routers and T Series routers, see Junos OS Administration Library, Configuring Junos OS to Support an External Clock Synchronization Interface for M Series, MX Series, and T Series Routers.

For information about configuring Synchronous Ethernet on MX 80, MX240, MX480, and MX960 Universal Routing Platforms, see Junos OS Administration Library, Synchronous Ethernet Overview and Configuring Clock Synchronization Interface on MX Series Routers.

Related Documentation
- Interface Alias Names Overview on page 107
- alias on page 418
- Configuring an External Synchronization Interface
- Configuring the Clock Source on page 113
**Configuring the Clock Source**

For both the router and interfaces, the clock source can be an external clock that is received on the interface or the router’s internal Stratum 3 clock.

To set the clock source as external or internal:

1. In configuration mode, go to the `edit interfaces interface-name` hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure the `clocking` option as external or internal.

   ```
   [edit interfaces interface-name]
   user@host# set clocking (external | internal)
   ```

---

**NOTE:** M7i and M10i routers do not support external clocking of SONET interfaces.

**NOTE:** On Channelized SONET/SDH PICs, if you set the parent (or the master) controller clock to external, then you must set the child controller clocks to the default value—that is, internal.

For example, on the Channelized STM1 PIC, if the clock on the Channelized STM1 interface (which is the master controller) is set to external, then you must not configure the CE1 interface (which is the child controller) clock to external. Instead you must configure the CE1 interface clock to internal.

For information about clocking on channelized interfaces, see *Channelized IQ and IQE Interfaces Properties*. Also see *Configuring the Clock Source on SONET/SDH Interfaces* and *Configuring the Channelized T3 Loop Timing*.

For information about configuring an external synchronization interface that can be used to synchronize the internal Stratum 3 clock to an external source on the M40e, M120, and M320 routers and on the T Series routers, see *Junos OS Administration Library, Configuring Junos OS to Support an External Clock Synchronization Interface for M Series, MX Series, and T Series Routers*.
For information about configuring Synchronous Ethernet on MX80, MX240, MX480, and MX960 Universal Routing Platforms, see Junos OS Administration Library, Synchronous Ethernet Overview and Configuring Clock Synchronization Interface on MX Series Routers.

**Related Documentation**
- Configuring an External Synchronization Interface
- clocking on page 472
- Clock Source Overview on page 112
- Configuring Junos OS to Support an External Clock Synchronization Interface for M Series, MX Series, and T Series Routers
- Synchronous Ethernet Overview
- Configuring Clock Synchronization Interface on MX Series Routers

**Configuring Interface Encapsulation on Physical Interfaces**

- Understanding Interface Encapsulation on Physical Interfaces on page 114
- Encapsulation Capabilities of Physical Interfaces on page 114
- Configuring the Encapsulation on a Physical Interface on page 115
- Displaying the Encapsulation on a Physical SONET/SDH Interface on page 116

**Understanding Interface Encapsulation on Physical Interfaces**

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default.

For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface. You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

**Encapsulation Capabilities of Physical Interfaces**

When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one `unit` statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point-to-point or multipoint.

Ethernet CCC encapsulation for Ethernet interfaces with standard TPID tagging requires that the physical interface have only a single logical interface. Ethernet interfaces in VLAN mode can have multiple logical interfaces.
For Ethernet interfaces in VLAN mode, VLAN IDs are applicable as follows:

- VLAN ID 0 is reserved for tagging the priority of frames.
- For encapsulation type `vlan-ccc`, VLAN IDs 1 through 511 are reserved for normal VLANs. VLAN IDs 512 and above are reserved for VLAN CCCs.
- For encapsulation type `vlan-vpls`, VLAN IDs 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 4094 are reserved for VPLS VLANs. For 4-port Fast Ethernet interfaces, you can use VLAN IDs 512 through 1024 for VPLS VLANs.
- For Gigabit Ethernet interfaces and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can configure flexible Ethernet services encapsulation on the physical interface. For interfaces with `flexible-ethernet-services` encapsulation, all VLAN IDs are valid. VLAN IDs from 1 through 511 are not reserved.
- For encapsulation types `extended-vlan-ccc` and `extended-vlan-vpls`, all VLAN IDs are valid.

The upper limits for configurable VLAN IDs vary by interface type.

When you configure a TCC encapsulation, some modifications are needed to handle VPN connections over unlike Layer 2 and Layer 2.5 links and terminate the Layer 2 and Layer 2.5 protocol locally.

The router performs the following media-specific changes:

- PPP TCC—Both Link Control Protocol (LCP) and Network Control Protocol (NCP) are terminated on the router. Internet Protocol Control Protocol (IPCP) IP address negotiation is not supported. The Junos OS strips all PPP encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to PPP encapsulation.
- Cisco HDLC TCC—Keepalive processing is terminated on the router. The Junos OS strips all Cisco HDLC encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to Cisco HDLC encapsulation.
- Frame Relay TCC—All Local Management Interface (LMI) processing is terminated on the router. The Junos OS strips all Frame Relay encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to Frame Relay encapsulation.
- ATM—Operation, Administration, and Maintenance (OAM) and Interim Local Management Interface (ILMI) processing is terminated at the router. Cell relay is not supported. The Junos OS strips all ATM encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to ATM encapsulation.

### Configuring the Encapsulation on a Physical Interface

By default, PPP is the encapsulation type for physical interfaces. To configure the encapsulation on a physical interface, include the encapsulation statement at the `[edit interfaces interface-name]` hierarchy level:
To configure encapsulation on a physical interface:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.
   ```
   [edit]
   user@host# set interfaces so-fpc/pic/port
   ```

2. Configure the encapsulation type as described in `encapsulation`.
   ```
   [edit interfaces mo-fpc/pic/port]
   user@host# set encapsulation encapsulation-type
   ```

   **NOTE:**
   - When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one unit statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point-to-point or multipoint.
   - When the encapsulation type is set to Cisco-compatible Frame Relay encapsulation, ensure that the LMI type is set to ANSI or Q933-A.
   - When `vlan-vpls` encapsulation is set at the physical interface level, commit check will validate that there should not be any inet family configured within it.

### Displaying the Encapsulation on a Physical SONET/SDH Interface

**Purpose**
To display the configured encapsulation and its associated set options on a physical interface when the following are set at the `[edit interfaces interface-name]` hierarchy level:

- `interface-name`—so-7/0/0
- Encapsulation—`ppp`
- Unit—0
- Family—`inet`
- Address—192.168.1.113/32
- Destination—192.168.1.114
- Family—`iso` and `mpls`

**Action**
Run the `show` command at the `[edit interfaces interface-name]` hierarchy level.

```
[edit interfaces so-7/0/0]
user@host# show encapsulation ppp:
```
unit 0 {
    point-to-point;
    family inet {
        address 192.168.1.113/32 {
            destination 192.168.1.114;
        }
    }
    family iso;
    family mpls;
}

**Meaning**
The configured encapsulation and its associated set options are displayed as expected. Note that the second set of two `family` statements allow IS-IS and MPLS to run on the interface.

**Related Documentation**
- encapsulation on page 571
- Configuring the Media MTU on page 99

## Configuring Interface Encapsulation on PTX Series Packet Transport Routers

This topic describes how to configure interface encapsulation on PTX Series Packet Transport Routers. Use the `flexible-ethernet-services` configuration statement to configure different encapsulation for different logical interfaces under a physical interface. With flexible Ethernet services encapsulation, you can configure each logical interface encapsulation without range restrictions for VLAN IDs.

Supported encapsulations for physical interfaces include:
- `flexible-ethernet-services`
- `ethernet-ccc`
- `ethernet-tcc`

Supported encapsulations for logical interfaces include:
- `ethernet`
- `vlan-ccc`
- `vlan-tcc`

---

**NOTE:** PTX Series Packet Transport Routers do not support extended-vlan-cc and extended-vlan-tcc encapsulation on logical interfaces. Instead, you can configure a tag protocol ID (TPID) value of 0x9100 to achieve the same results.
To configure flexible Ethernet services encapsulation, include the `encapsulation flexible-ethernet-services` statement at the `[edit interfaces et-fpc/pic/port]` hierarchy level. For example:

```conf
interfaces {
  et-fpc/pic/port {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
      vlan-id 1000;
      family inet {
        address 11.0.0.20/24;
      }
    }
    unit 1 {
      encapsulation vlan-ccc;
      vlan-id 1010;
    }
    unit 2 {
      encapsulation vlan-tcc;
      vlan-id 1020;
      family tcc {
        proxy {
          inet-address 11.0.2.160;
        }
        remote {
          inet-address 11.0.2.10;
        }
      }
    }
  }
}
```

Related Documentation

- Configuring Interface Encapsulation on Physical Interfaces on page 114

**Configuring Keepalives**

By default, physical interfaces configured with Cisco HDLC or PPP encapsulation send keepalive packets at 10-second intervals. The Frame Relay term for keepalives is LMI packets; the Junos OS supports both ANSI T1.617 Annex D LMIs and ITU Q933 Annex A LMIs. On ATM networks, OAM cells perform the same function. You configure OAM cells at the logical interface level; for more information, see Defining the ATM OAM F5 Loopback Cell Period.

To disable the sending of keepalives:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   ```conf
   [edit]
   user@host# edit interfaces interface-name
   ```
2. Include the `no-keepalives` statement at the `[edit interfaces interface-name]` hierarchy level.

   [edit interfaces interface-name]
   no-keepalives;

To disable the sending of keepalives on a physical interface configured with Cisco HDLC encapsulation for a translational cross-connection:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   [edit ]
   user@host# edit interfaces interface-name

2. Include the `no-keepalives` statement with the `encapsulation cisco-hdlc-tcc` statement at the `[edit interfaces interface-name]` hierarchy level.

   [edit interfaces interface-name]
   encapsulation cisco-hdlc-tcc;
   no-keepalives;

To disable the sending of keepalives on a physical interface configured with PPP encapsulation for a translational cross-connection:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   [edit ]
   user@host# edit interfaces interface-name

2. Include the `no-keepalives` statement with the `encapsulation ppp-tcc` statement at the `[edit interfaces interface-name]` hierarchy level.

   [edit interfaces interface-name]
   encapsulation ppp-tcc;
   no-keepalives;

For more information about translation cross-connections, see Circuit and Translational Cross-Connects Overview.

When you configure PPP over ATM or Multilink PPP over ATM encapsulation, you can enable or disable keepalives on the logical interface. For more information, see Configuring PPP over ATM2 Encapsulation.

To explicitly enable the sending of keepalives:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   [edit ]
user@host# edit interfaces interface-name

2. Include the `keepalives` statement at the `[edit interfaces interface-name]` hierarchy level.

   ```
   [edit interfaces interface-name]
   keepalives;
   ```

To change one or more of the default keepalive values:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level.

   ```
   [edit ]
   user@host# edit interfaces interface-name
   ```

2. Include the `keepalives` statement with the appropriate option as `interval seconds`, `down-count number`, and the `up-count number`:

   ```
   [edit interfaces interface-name]
   keepalives;
   keepalives <interval seconds> <down-count number> <up-count number>;
   ```

On interfaces configured with Cisco HDLC or PPP encapsulation, you can include the following three keepalive statements; note that Frame Relay encapsulation is not affected by these statements:

- **interval seconds**—The time in seconds between successive keepalive requests. The range is from 1 second through 32767 seconds, with a default of 10 seconds.

- **down-count number**—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is from 1 through 255, with a default of 3.

- **up-count number**—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is from 1 through 255, with a default of 1.

---

**CAUTION:** If interface keepalives are configured on an interface that does not support the `keepalives` configuration statement (for example, 10-Gigabit Ethernet), the link layer may go down when the PIC is restarted. Avoid configuring the keepalives on interfaces that do not support the `keepalives` configuration statement.

---

For information about Frame Relay keepalive settings, see Configuring Frame Relay Keepalives.
On MX Series routers with Modular Port Concentrators/Modular Interface Cards (MPCs/MICs), the Packet Forwarding Engine on an MPC/MIC processes and responds to Link Control Protocol (LCP) Echo-Request keepalive packets that the PPP subscriber (client) initiates and sends to the router. The mechanism by which LCP Echo-Request packets are processed by the Packet Forwarding Engine instead of by the Routing Engine is referred to as **PPP fast keepalive**. For more information about how PPP fast keepalive works on an MX Series router with MPCs/MICs, see the *Junos OS Subscriber Access Configuration Guide*.

**Related Documentation**
- *Defining the ATM OAM F5 Loopback Cell Period*
- *Disabling the Sending of PPPoE Keepalive Messages*
  - *Understanding How the Router Processes Subscriber-Initiated PPP Fast Keepalive Requests*
  - **keepalives on page 718**
  - **no-keepalives on page 832**
- *Configuring Frame Relay Keepalives*
- *Circuit and Translational Cross-Connects Overview on page 255*
- *Configuring PPP over ATM2 Encapsulation Overview*

### Configuring the PPP Challenge Handshake Authentication Protocol

- *PPP Challenge Handshake Authentication Protocol on page 121*
- *Configuring the PPP Challenge Handshake Authentication Protocol on page 121*
- *Displaying the Configured PPP Challenge Handshake Authentication Protocol on page 123*

#### PPP Challenge Handshake Authentication Protocol

For interfaces with PPP encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP), as defined in RFC 1994, **PPP Challenge Handshake Authentication Protocol (CHAP)**. When you enable CHAP on an interface, the interface can authenticate its peer and can be authenticated by its peer. By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges. To enable CHAP, you must create an access profile, and you must configure the interfaces to use CHAP.

#### Configuring the PPP Challenge Handshake Authentication Protocol

When you configure an interface to use CHAP, you must assign an access profile to the interface. When an interface receives CHAP challenges and responses, the access profile in the packet is used to look up the shared secret, as defined in RFC 1994. If no matching access profile is found for the CHAP challenge that was received by the interface, the optionally configured default CHAP secret is used. The default CHAP secret is useful if the CHAP name of the peer is unknown, or if the CHAP name changes during PPP link negotiation.
To enable CHAP, you must create an access profile, and you must configure the interfaces to use PAP. For more information on how to configure access profile, see Configuring Access Profiles for L2TP or PPP Parameters.

To configure the PPP challenge handshake authentication protocol, on each physical interface with PPP encapsulation, perform the following steps.

1. To assign an access profile to an interface, include the `access-profile` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level.

```
[edit interfaces interface-name ppp-options chap]
user@host# set access-profile name
```

**NOTE:** You must include the `access-profile` statement when you configure the CHAP authentication method. If an interface receives a CHAP challenge or response from a peer that is not in the applied access profile, the link is immediately dropped unless a default CHAP secret has been configured.

2. The default CHAP secret is used when no matching CHAP access profile exists, or if the CHAP name changes during PPP link negotiation. To configure a default CHAP secret for an interface, include the `default-chap-secret` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level.

```
[edit interfaces interface-name ppp-options chap]
user@host# set default-chap-secret name
```

3. To configure the name the interface uses in CHAP challenge and response packets, include the `local-name` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level:

```
[edit interfaces interface-name ppp-options chap]
user@host# set local-name name
```

**NOTE:**
- The local name is any string from 1 through 32 characters in length, starting with an alphanumeric or underscore character, and including only the following characters:
  
  `a-zA-Z 0-9 % @ / \ _ -`

- By default, when CHAP is enabled on an interface, the interface uses the router's system hostname as the name sent in CHAP challenge and response packets.
4. You can configure the interface not to challenge its peer, and only respond when challenged. To configure the interface not to challenge its peer, include the `passive` statement at the `[edit interfaces interface-name ppp-options chap]` hierarchy level:

```bash
[edit interfaces interface-name ppp-options chap]
user@host# set passive;
```

**NOTE:** By default, when CHAP is enabled on an interface, the interface always challenges its peer and responds to challenges from its peer.

**See Also**
- Configuring the PPP Authentication Protocol

### Displaying the Configured PPP Challenge Handshake Authentication Protocol

**Purpose**
To display the configured PPP CHAP at the `[edit access]` and `[edit interfaces]` hierarchy levels.

- Access profile—`pe-A-ppp-clients`
- default CHAP secret data—"$ABC123"
- hostname for the CHAP challenge and response packets—"pe-A-so-1/1/1"
- Interface—so-1/1/2

**Action**
- Run the `show` command at the `[edit access]` hierarchy level.

```bash
profile pe-A-ppp-clients;
client cpe-1 chap-secret "$ABC123";
# SECRET-DATA
[edit interfaces so-1/2/0]
encapsulation ppp;
ppp-options {
  chap {
    access-profile pe-A-ppp-clients;
    default-chap-secret "$ABC123";
    local-name "pe-A-so-1/1/1";
  }
}
```

- Run the `show` command at the `[edit interfaces s0-1/1/2]` hierarchy level.

```bash
ppp-options {
  chap {
    access-profile pe-A-ppp-clients;
    default-chap-secret "$ABC123";
    local-name "pe-A-so-1/1/2";
  }
}
```
Meaning  The configured CHAP and its associated set options are displayed as expected.

Configuring the PPP Password Authentication Protocol On a Physical Interface

- Understanding PPP Password Authentication Protocol on page 124
- Configuring the PPP Password Authentication Protocol On a Physical Interface on page 124
- Configuring the PPP Password Authentication Protocol On a Logical Interface on page 126

Understanding PPP Password Authentication Protocol

For interfaces with PPP encapsulation, you can configure interfaces to support the Password Authentication Protocol (PAP), as defined in RFC 1334, PAP Authentication Protocols. If authentication is configured, the PPP link negotiates using CHAP or PAP protocol for authentication during the Link Control Protocol (LCP) negotiation phase. PAP is only performed after the link establishment phase (LCP up) portion of the authentication phase.

During authentication, the PPP link sends a PAP authentication-request packet to the peer with an ID and password. The authentication-request packet is sent every 2 seconds, similar to the CHAP challenge, until a response is received (acknowledgment packet, nonacknowledgment packet). If an acknowledgment packet is received, the PPP link transitions to the next state, the network phase. If a nonacknowledgment packet is received, an LCP terminate request is sent, and the PPP link goes back to the link establishment phase. If no response is received, and an optional retry counter is set to true, a new request acknowledgment packet is resent. If the retry counter expires, the PPP link transitions to the LCP negotiate phrase.

You can configure the PPP link with PAP in passive mode. By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation—in passive mode, the interface does not authenticate the peer.

Configuring the PPP Password Authentication Protocol On a Physical Interface

When you configure an interface to use PAP, you must assign an access profile to the interface. When an interface receives PAP authentication requests, the access profile in the packet is used to look up the password.

To enable PAP, you must create an access profile, and you must configure the interfaces to use PAP. For more information on how to configure access profile, see Configuring Access Profiles for L2TP or PPP Parameters.
To configure the PPP password authentication protocol, on each physical interface with PPP encapsulation, perform the following steps.

1. To assign an access profile to an interface, include the `access-profile` statement at the `[edit interfaces interface-name ppp-options pap]` hierarchy level.

```
[edit interfaces interface-name ppp-options pap]
user@host# set access-profile name
```

2. To configure the name the interface uses in PAP request and response packets, include the `local-name` statement at the `[edit interfaces interface-name ppp-options pap]` hierarchy level:

```
[edit interfaces interface-name ppp-options pap]
user@host# set local-name name
```

3. You need to configure the password to be used for authentication. To configure the host password for sending PAP requests, include the `local-password` statement at the `[edit interfaces interface-name ppp-options pap]` hierarchy level:

```
[edit interfaces interface-name ppp-options pap]
user@host# set local-password password
```

   **NOTE:** By default, when PAP is enabled on an interface, the interface uses the router’s system hostname as the name sent in PAP request and response packets.

4. To configure the interface to authenticate with PAP in passive mode, include the `passive` statement at the `[edit interfaces interface-name ppp-options pap]` hierarchy level:

```
[edit interfaces interface-name ppp-options pap]
user@host# set passive
```

   **NOTE:** By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation—in passive mode, the interface does not authenticate the peer.

**See Also**  
- *Configuring the PPP Authentication Protocol*
Configuring the PPP Password Authentication Protocol On a Logical Interface

When you configure an interface to use PAP, you must assign an access profile to the interface. When an interface receives PAP authentication requests, the access profile in the packet is used to look up the password. If no matching access profile is found for the PAP authentication request that was received by the interface, the optionally configured default PAP password is used.

To configure the PPP password authentication protocol, on each logical interface with PPP encapsulation, perform the following steps.

1. To configure the default PAP password, include the `pap-password` statement at the
   `[edit interfaces interface-name unit logical-unit-number ppp-options pap]` hierarchy level:

   ```
   [edit interfaces interface-name unit logical-unit-number ppp-options pap]
   user@host# set default-pap-password password
   ```

2. To configure the name the interface uses in PAP request and response packets, include
   the `local-name` statement at the `[edit interfaces interface-name unit logical-unit-number
   ppp-options pap]` hierarchy level:

   ```
   [edit interfaces interface-name ppp-options pap]
   user@host# set local-name name
   ```

3. You need to configure the password to be used for authentication. To configure the
   host password for sending PAP requests, include the `local-password` statement at
   the `[edit interfaces interface-name ppp-options pap]` hierarchy level:

   ```
   [edit interfaces interface-name unit logical-unit-number ppp-options pap]
   user@host# set local-password password
   ```

   **NOTE:** By default, when PAP is enabled on an interface, the interface uses
   the router's system hostname as the name sent in PAP request and
   response packets.

4. To configure the interface to authenticate with PAP in passive mode, include the
   `passive` statement at the `[edit interfaces interface-name unit logical-unit-number
   ppp-options pap]` hierarchy level:

   ```
   [edit interfaces interface-name unit logical-unit-number ppp-options pap]
   user@host# set passive
   ```
NOTE: By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation—in passive mode, the interface does not authenticate the peer.

See Also

• Configuring the PPP Authentication Protocol

PPP Encapsulation on ACX Series Routers

You can configure Point-to-Point Protocol (PPP) encapsulation on physical interfaces on ACX Series routers. PPP provides a standard method for transporting multiprotocol datagrams over a point-to-point link. PPP uses the High-Speed Data Link Control (HDLC) protocol for its physical interface and provides a packet-oriented interface for the network-layer protocols.

PPP is supported on the following MICs on ACX Series routers:

• On ACX1000 routers with 8-port built-in T1/E1 TDM MICs.
• On ACX2000, ACX2100, ACX2200, and ACX4000 routers with 16-port built-in T1/E1 TDM MICs.
• On ACX4000 routers with 16-Port Channelized E1/T1 Circuit Emulation MICs.

Starting with Release 12.3X54, you can configure Point-to-Point Protocol (PPP) encapsulation on physical interfaces on Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP on ACX4000 Series routers.

On ACX Series routers, E1, T1, and NxDS0 interfaces support PPP encapsulation.

PPP is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface.

To configure the encapsulation on a physical interface, include the encapsulation ppp statement at the [edit interfaces interface-name] hierarchy level.

IP class of service (CoS) is not supported on PPP interfaces. All the traffic is sent to the best effort queue (queue 0) and CoS code points are not processed. Also, fixed classifiers are not supported. Circuit cross-connect (CCC) version of PPP (ppp-ccc option) and translational cross-connect (TCC) version of PPP (ppp-tcc option) are not supported for configuration with the encapsulation statement.
PPP is supported only for IPv4 networks. If you configure PPP encapsulation, you can configure an INET family by including the family inet statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level. MPLS family is not supported on logical interfaces if you configured PPP encapsulation. On interfaces with PPP encapsulation, configure PPP-specific interface properties by including the ppp-options statement at the [edit interfaces interface-name] hierarchy level. For interfaces with PPP encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

For full T1/E1 interfaces on which PPP encapsulation needs to be enabled, create the T1/E1 interfaces out of channelized T1/E1 interfaces (CT1/CE1) by including the framing statement at the [edit chassis fpc fpc-slot pic pic-slot] hierarchy level:

```
[edit chassis fpc fpc-slot pic pic-slot]
user@host# set framing (t1 | e1);
```

Configure a CT1 port down to a T1 channel. On the CT1 interface, set the no-partition option and then set the interface type as T1.

```
[edit interfaces ct1-fpc-slot/mic-slot/port-number]
user@host# set no-partition interface-type t1
```

Configure a CE1 port down to an E1 channel. On the CE1 interface, set the no-partition option and then set the interface type as E1.

```
[edit interfaces ce1-fpc-slot/mic-slot/port-number]
user@host# set no-partition interface-type e1
```

For NxDS0 interfaces on which PPP encapsulation needs to be enabled, partition the CE1 and CT1 interfaces by including the cel-x/y/z partition partition-number timeslots interface-type ds and ct1-x/y/z partition partition-number timeslots interface-type ds statements at the [edit interfaces interface-name] hierarchy level.

The following operational mode commands can be used to view PPP configuration settings and statistical details:

- The show ppp address-pool command is used to display PPP address pool information.
- The show ppp interface command is used to display PPP session information for an interface.
- The show ppp statistics command is used to display PPP session statistics.
- The show ppp summary command is used to display summary information about PPP-configured interfaces.
- The show interfaces e1-fpc/pic/port, show interfaces t1-fpc/pic/port, and show interfaces ds-fpc/pic/port commands are used to display the PPP settings of a specific E1, T1, and DS interface, respectively.

Related Documentation

- Configuring Interface Encapsulation on Physical Interfaces in ACX Series on page 129
Configuring Interface Encapsulation on Physical Interfaces in ACX Series

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface.

You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types. For more information about logical interface encapsulation, see Configuring Interface Encapsulation on Logical Interfaces.

This section contains the following topics:

- Configuring the Encapsulation on a Physical Interface on page 129
- Encapsulation Capabilities on page 131

Configuring the Encapsulation on a Physical Interface

By default, PPP is the encapsulation type for physical interfaces. To configure the encapsulation on a physical interface, include the `encapsulation` statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
```

**NOTE:** ACX Series routers do not support `cisco-hdlc` encapsulation.

The physical interface encapsulation can be one of the following:

- **ATM CCC cell relay**—Connects two remote virtual circuits or ATM physical interfaces with a label-switched path (LSP). Traffic on the circuit is ATM cells.
  
  For more information, see the Junos OS Administration Library.

- **ATM PVC**—Defined in RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5. When you configure physical ATM interfaces with ATM PVC encapsulation, an RFC 2684-compliant ATM Adaptation Layer 5 (AAL5) tunnel is set up to route the
ATM cells over a Multiprotocol Label Switching (MPLS) path that is typically established between two MPLS-capable routers using the Label Distribution Protocol (LDP).

- Ethernet cross-connect—Ethernet interfaces without VLAN tagging can use Ethernet CCC encapsulation. Two related versions are supported:
  - CCC version (ethernet-ccc)—Ethernet interfaces with standard Tag Protocol ID (TPID) tagging can use Ethernet CCC encapsulation. When you use this encapsulation type, you can configure the ccc family only.
  - TCC version (ethernet-tcc)—Similar to CCC, but used for circuits with different media on either side of the connection.

  For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC is not supported.

- VLAN CCC (vlan-ccc)—Ethernet interfaces with VLAN tagging enabled can use VLAN CCC encapsulation. VLAN CCC encapsulation supports TPID 0x8100 only. When you use this encapsulation type, you can configure the ccc family only.

- Extended VLAN cross-connect—Gigabit Ethernet interfaces with VLAN 802.1Q tagging enabled can use extended VLAN cross-connect encapsulation. (Ethernet interfaces with standard TPID tagging can use VLAN CCC encapsulation.) Two related versions of extended VLAN cross-connect are supported:
  - CCC version (extended-vlan-ccc)—Extended VLAN CCC encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. When you use this encapsulation type, you can configure the ccc family only.
  - TCC version (extended-vlan-tcc)—Similar to CCC, but used for circuits with different media on either side of the connection.

  For 8-port, 12-port, and 48-port Fast Ethernet PICs, extended VLAN CCC is not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC and extended VLAN TCC are not supported.

  **NOTE:** In ACX Series routers, VPLS is supported only on ACX5048 and ACX5096 routers.

- Ethernet VPLS (ethernet-vpls)—Ethernet interfaces with VPLS enabled can use Ethernet VPLS encapsulation. For more information about VPLS, see the Junos OS VPNs Library for Routing Devices.

- Ethernet VLAN VPLS (vlan-vpls)—Ethernet interfaces with VLAN tagging and VPLS enabled can use Ethernet VLAN VPLS encapsulation. For more information about VPLS, see the Junos OS VPNs Library for Routing Devices.

- Extended VLAN VPLS (extended-vlan-vpls)—Ethernet interfaces with VLAN 802.1Q tagging and VPLS enabled can use Ethernet Extended VLAN VPLS encapsulation. (Ethernet interfaces with standard TPID tagging can use Ethernet VLAN VPLS encapsulation.) Extended Ethernet VLAN VPLS encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. For more information about VPLS, see the Junos OS VPNs Library for Routing Devices.
Flexible Ethernet services (flexible-ethernet-services)—Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router) can use flexible Ethernet services encapsulation. Aggregated Ethernet bundles can use this encapsulation type. You use this encapsulation type when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of route, TCC, CCC, Layer 2 virtual private networks (VPNs), and VPLS encapsulations on a single physical port. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

PPP—Defined in RFC 1661, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*. PPP is the default encapsulation type for physical interfaces. E1, E3, SONET/SDH, T1, and T3 interfaces can use PPP encapsulation.

**NOTE:** When the encapsulation type is set to Cisco-compatible Frame Relay encapsulation, ensure that the LMI type is set to ANSI or Q933-A.

In ACX Series routers, VPLS is supported only on ACX5048 and ACX5096 routers.

**Encapsulation Capabilities**

When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one `unit` statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point-to-point or multipoint.

Ethernet CCC encapsulation for Ethernet interfaces with standard TPID tagging requires that the physical interface have only a single logical interface. Ethernet interfaces in VLAN mode can have multiple logical interfaces.

For Ethernet interfaces in VLAN mode, VLAN IDs are applicable as follows:

- VLAN ID 0 is reserved for tagging the priority of frames.
- For encapsulation type `vlan-ccc`, VLAN IDs 1 through 511 are reserved for normal VLANs. VLAN IDs 512 and above are reserved for VLAN CCCs.

When you configure Ethernet virtual LAN (VLAN) encapsulation on CCC circuits (by using the `encapsulation vlan-ccc` statement at the `[edit interfaces interface-name]` hierarchy level), you can bind a list of VLAN IDs to the interface by using the `vlan-id-list [ vlan-id-numbers ]` statement to configure a CCC for multiple VLANs. Configuring this statement creates a CCC for:

- Each VLAN listed—for example, `vlan-id-list [ 100 200 300 ]`
- Each VLAN in a range—for example, `vlan-id-list [ 100-200 ]`
Each VLAN in a list and range combination—for example, `vlan-id-list [50, 100-200, 300]`

• For encapsulation type `vlan-vpls`, VLAN IDs 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 4094 are reserved for VPLS VLANs. For 4-port Fast Ethernet interfaces, you can use VLAN IDs 512 through 1024 for VPLS VLANs.

• For Gigabit Ethernet interfaces and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), you can configure flexible Ethernet services encapsulation on the physical interface. For interfaces with `flexible-ethernet-services` encapsulation, all VLAN IDs are valid. VLAN IDs from 1 through 511 are not reserved.

• For encapsulation types `extended-vlan-ccc` and `extended-vlan-vpls`, all VLAN IDs are valid.

The upper limits for configurable VLAN IDs vary by interface type.

When you configure a TCC encapsulation, some modifications are needed to handle VPN connections over unlike Layer 2 and Layer 2.5 links and terminate the Layer 2 and Layer 2.5 protocol locally.

The router performs the following media-specific change:

• ATM—Operation, Administration, and Maintenance (OAM) and Interim Local Management Interface (ILMI) processing is terminated at the router. Cell relay is not supported. The Junos OS strips all ATM encapsulation data from incoming frames before forwarding them. For output, the next hop is changed to ATM encapsulation.

**Example: Configuring the Encapsulation on a Physical Interface**

Configure PPP encapsulation on a SONET/SDH interface. The second and third `family` statements allow Intermediate System-to-Intermediate System (IS-IS) and MPLS to run on the interface.

```plaintext
[edit interfaces]
so-7/0/0 {
  encapsulation ppp;
  unit 0 {
    point-to-point;
    family inet {
      address 192.168.1.113/32 {
        destination 192.168.1.114;
      }
    }
    family iso;
    family mpls;
  }
}
```

**Related Documentation**

- Configuring Interface Encapsulation on Logical Interfaces
Configuring PPP Address and Control Field Compression

For interfaces with PPP, PPP CCC, or PPP TCC encapsulation, you can configure compression of the Data Link Layer address and control fields, as defined in RFC 1661, *The Point-to-Point Protocol (PPP)*. By default, the address and control fields are not compressed. This means PPP-encapsulated packets are transmitted with two 1-byte fields (0xff and 0x03). If you configure address and control field compression (ACFC) and ACFC is successfully negotiated with the local router’s peer, the local router transmits packets without these 2 bytes. ACFC allows you to conserve bandwidth by transmitting less data.

On M320, M120, and T Series routers, ACFC is not supported for any ISO family protocols. Do not include the `acfc` statement at the `[edit interfaces interface-name ppp-options]` hierarchy level when you include the `family iso` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

**NOTE:** The address and control fields cannot be compressed in Link Control Protocol (LCP) packets.

The PPP session restarts when you configure or modify compression options.

To configure ACFC:

1. In configuration mode, go to the `[edit interfaces interface-name ppp-options]` hierarchy level.

   ```
   [edit ]
   user@host# edit interfaces interface-name ppp-options
   ```

2. Include the `compression` statement at the `[edit interfaces interface-name ppp-options]` hierarchy level, and specify `acfc`.

   ```
   [edit interfaces interface-name ppp-options]
   compression acfc;
   ```

To monitor the configuration, issue the `show interfaces interface-name` command. Configured options are displayed in the `link flags` field for the physical interface. Successfully negotiated options are displayed in the `flags` field for the logical interface. In this example, both ACFC and PFC are configured, but neither compression feature has been successfully negotiated.

```
user@router# run show interfaces so-0/1/1
Physical interface: so-0/1/1, Enabled, Physical link is Up
   Interface index: 133, SNMP ifIndex: 27
   Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
   Loopback: None, FCS: 16
   Payload scrambler: Enabled
```
This configuration causes the local router to try to negotiate ACFC with its peer. If ACFC is successfully negotiated, the local router sends packets with compressed address and control fields. When you include the `compression acfc` statement in the configuration, the PPP session restarts, and the local router sends the ACFC option in the LCP Configure-Request packet. The ACFC option informs the local router's peer that the local router can receive packets with compression. If the peer indicates that it, too, can receive packets with compression, then ACFC is negotiated. If ACFC is successfully negotiated, the local router can receive packets with or without the address and control bytes included.

**Related Documentation**

- ppp-options on page 910
- compression on page 478
- acfc on page 397
Configuring the PPP Protocol Field Compression

For interfaces with PPP, PPP CCC, or PPP TCC encapsulation, you can configure protocol field compression. By default, the protocol field is not compressed. This means PPP-encapsulated packets are transmitted with a two-byte protocol field. For example, IPv4 packets are transmitted with the protocol field set to 0x0021, and MPLS packets are transmitted with the protocol field set to 0x0281.

For all protocols with identifiers in the range 0x0000 through 0x00ff, you can configure the router to compress the protocol field to one byte, as defined in RFC 1661, The Point-to-Point Protocol (PPP). Protocol field compression (PFC) allows you to conserve bandwidth by transmitting less data.

NOTE: The protocol field cannot be compressed in Link Control Protocol (LCP) packets.

The PPP session restarts when you configure or modify compression options.

To configure PFC:

1. In configuration mode, go to the [edit interfaces interface-name ppp-options] hierarchy level.

   [edit]
   user@host# edit interfaces interface-name ppp-options

2. Include the compression statement at the [edit interfaces interface-name ppp-options] hierarchy level, and specify pfc.

   [edit interfaces interface-name ppp-options]
   compression pfc;

To monitor the configuration, issue the show interfaces interface-name command. Configured options are displayed in the link flags field for the physical interface. Successfully negotiated options are displayed in the flags field for the logical interface. In this example, both ACFC and PFC are configured, but neither compression feature has been successfully negotiated.

user@router# run show interfaces so-0/1/1

Physical interface: so-0/1/1, Enabled, Physical link is Up
Interface index: 133, SNMP ifIndex: 27
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3, Loopback: None, FCS: 16,
Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps 16384
Link flags : No-Keepalives ACFC PFC
LCP state: Opened
This configuration causes the local router to try to negotiate PFC with its peer. If PFC is successfully negotiated, the local router sends packets with compressed protocol fields. When you include the `compression pfc` statement in the configuration, the PPP session restarts, and the local router sends the PFC option in the LCP Configure-Request packet. The PFC option informs the local router’s peer that the local router can receive packets with compression. If the peer indicates that it, too, can receive packets with compression, then PFC is negotiated. If PFC is successfully negotiated, the local router can receive packets with either 2-byte (uncompressed) or 1-byte (compressed) protocol fields.

### Related Documentation
- ppp-options on page 910
- compression on page 478
- pfc on page 887

### Monitoring a PPP Session

You can monitor PPP packet exchanges. When monitoring is enabled, packets exchanged during a session are logged by default to `/var/log/pppd`, or to the file specified in the `traceoptions` statement.

To monitor a PPP session:

1. In configuration mode, go to the `[edit protocols ppp]` hierarchy level.

   ```
   [edit]
   user@host# edit protocols ppp
   ```

2. Include the `monitor-session` statement.

   ```
   [edit protocols ppp]
   user@host# monitor-session (interface-name | all);
   ```
When monitoring is configured, the operational mode commands `show ppp summary` and `show ppp interface` display a Monitored flag in the Session flags column or line.

Related Documentation: `monitor-session` on page 794

### Tracing Operations of the pppd Process

You can trace the operations of the router's pppd process.

To trace the router's pppd process:

1. In configuration mode, go to the `[edit protocols ppp]` hierarchy level.

   ```
   [edit ]
   user@host# edit protocols ppp
   ```

2. Include the `traceoptions` statement.

   ```
   [edit protocols ppp]
   traceoptions {
   file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>; flag flag; level severity-level; no-remote-trace;
   }
   ```

   - To specify more than one tracing operation, include multiple `flag` statements.

   You can specify the following flags in the `traceoptions` statement:

   - **access**—Trace access code
   - **address-pool**—Trace address pool code
   - **all**—Trace all areas of code
   - **auth**—Trace authentication code
   - **chap**—Trace challenge handshake authentication protocol code
   - **ci**—Trace CI code
   - **config**—Trace configuration code
   - **ifdb**—Trace interface database code
   - **lcp**—Trace LCP state machine code
   - **memory**—Trace memory management code
   - **message**—Trace message processing code
   - **mlppp**—Trace multilink point-to-point protocol code
By default, when you configure an interface with Frame Relay encapsulation, the routing platform is assumed to be data terminal equipment (DTE). That is, the routing platform is assumed to be at a terminal point on the network.

When you configure the router to be a data circuit-terminating equipment (DCE), keepalives are disabled by default.

To configure the router to be DCE:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure the dce option to respond to Frame Relay status enquiry messages.

   ```
   [edit interfaces interface-name]
   user@host# set dce
   ```

Perform one of the following tasks for back-to-back Frame Relay connections:

- Disable sending of keepalives on both sides of the connection.

- Configure one side of the connection as a DTE (the default Junos configuration) by removing the dce statement from the configuration and the other as a DCE.
Receive and Transmit Leaky Bucket Properties Overview

Congestion control is particularly difficult in high-speed networks with high volumes of traffic. When congestion occurs in such a network, it is usually too late to react. You can avoid congestion by regulating the flow of packets into your network. Smoother flows prevent bursts of packets from arriving at (or being transmitted from) the same interface and causing congestion.

For all interface types except ATM, Fast Ethernet, Gigabit Ethernet, and channelized IQ and IQE, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on and transmitted by a particular interface. You effectively specify what percentage of the interface's total capacity can be used to receive or transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit high volumes of traffic.

**NOTE:** Instead of configuring leaky bucket properties, you can limit traffic flow by configuring policers. Policers work on all interfaces. For more information, see the [Routing Policies, Firewall Filters, and Traffic Policers Feature Guide](#).

The leaky bucket is used at the host-network interface to allow packets into the network at a constant rate. Packets might be generated in a bursty manner, but after they pass through the leaky bucket, they enter the network evenly spaced. In some cases, you might want to allow short bursts of packets to enter the network without smoothing them out. By controlling the number of packets that can accumulate in the bucket, the threshold property controls burstiness. The maximum number of packets entering the network in time units is $threshold + rate * t$.

By default, leaky buckets are disabled and the interface can receive and transmit packets at the maximum line rate.

For each DS3 channel on a channelized OC12 interface, you can configure unique receive and transmit buckets.

**NOTE:** HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the Junos OS rejects configurations that have both features enabled. For more information, see [Configuring SONET/SDH HDLC Payload Scrambling for Link Stability](#).

---

### Related Documentation
- [dce on page 503](#)
- [Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140](#)
- [SONET/SDH Interfaces Overview](#)
• receive-bucket on page 948
• transmit-bucket on page 1076

Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion

You can configure leaky bucket properties which allow you to limit the amount of traffic received on and transmitted by a particular interface. You can specify what percentage of the interface’s total capacity can be used to receive or transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit high volumes of traffic.

To configure leaky bucket properties:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level.

   [edit]
   user@host# edit interfaces interface-name

2. Configure the receive-bucket statement.

   [edit interfaces interface-name]
   user@host# set receive-bucket

3. Configure the overflow option, the threshold option, and the rate option for the receive leaky bucket, which specifies what percentage of the interface’s total capacity can be used to receive packets.

   [edit interfaces interface-name receive-bucket]
   user@host# set overflow (discard | tag)
   user@host# set threshold bytes
   user@host# set rate percentage

4. Configure the transmit-bucket statement.

   [edit interfaces interface-name]
   user@host# set transmit-bucket

5. Configure the overflow option, the threshold option, and the rate option for the transmit leaky bucket, which specifies what percentage of the interface’s total capacity can be used to transmit packets.

   [edit interfaces interface-name transmit-bucket]
   user@host# set overflow (discard | tag)
   user@host# set threshold bytes
   user@host# set rate percentage
Understanding Unidirectional Traffic Flow on Physical Interfaces

By default, physical interfaces are bidirectional; that is, they both transmit and receive traffic. You can configure unidirectional link mode on a 10-Gigabit Ethernet interface that creates two new physical interfaces that are unidirectional. The new transmit-only and receive-only interfaces operate independently, but both are subordinate to the original parent interface.

The unidirectional interfaces enable the configuration of a unidirectional link topology. Unidirectional links are useful for applications such as broadband video services where almost all traffic flow is in one direction, from the provider to the user. Unidirectional link mode conserves bandwidth by enabling it to be differentially dedicated to transmit and receive interfaces. In addition, unidirectional link mode conserves ports for such applications because the transmit-only and receive-only interfaces act independently. Each can be connected to different routers, for example, reducing the total number of ports required.

NOTE: Unidirectional link mode is currently supported on only the following hardware:

- 4-port 10-Gigabit Ethernet DPC on the MX960 router
- 10-Gigabit Ethernet IQ2 PIC and 10-Gigabit Ethernet IQ2E PIC on the T Series router

The transmit-only interface is always operationally up. The operational status of the receive-only interface depends only on local faults; it is independent of remote faults and of the status of the transmit-only interface.

On the parent interface, you can configure attributes common to both interfaces, such as clocking, framing, gigether-options, and sonet-options. On each of the unidirectional interfaces, you can configure encapsulation, MAC address, MTU size, and logical interfaces.

Unidirectional interfaces support IP and IPv6. Packet forwarding takes place by means of static routes and static ARP entries, which you can configure independently on both unidirectional interfaces.

Only transmit statistics are reported on the transmit-only interface (and shown as zero on the receive-only interface). Only receive statistics are reported on the receive-only interface (and shown as zero on the transmit-only interface). Both transmit and receive statistics are reported on the parent interface.
Enabling Unidirectional Traffic Flow on Physical Interfaces

By default, physical interfaces are bidirectional; that is, they both transmit and receive traffic. You can configure unidirectional link mode on a 10-Gigabit Ethernet interface that creates two new physical interfaces that are unidirectional. The new transmit-only and receive-only interfaces operate independently, but both are subordinate to the original parent interface.

To enable unidirectional link mode on a physical interface, perform the following steps:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level:

```
[edit]
user@host# edit interfaces interface-name
```

2. Configure the unidirectional option to create two new, unidirectional (transmit-only and receive-only) physical interfaces subordinate to the original parent interface.

```
[edit interfaces interface-name]
user@host# set unidirectional
```

**NOTE:** Unidirectional link mode is currently supported on only the following hardware:

- 4-port 10–Gigabit Ethernet DPC on the MX960 router
- 10–Gigabit Ethernet IQ2 PIC and 10–Gigabit Ethernet IQ2E PIC on the T Series router

Related Documentation

- unidirectional on page 1090
- Enabling Unidirectional Traffic Flow on Physical Interfaces on page 142
Physical Interface Damping Overview

Physical interface damping limits the advertisement of the up and down transitions (flapping) on an interface. Each time a transition occurs, the interface state is changed, which generates an advertisement to the upper-level routing protocols. Damping helps reduce the number of these advertisements.

From the viewpoint of network deployment, physical interface flaps fall into the following categories:

- Nearly instantaneous multiple flaps of short duration (milliseconds).
- Periodic flaps of long duration (seconds).

Figure 6 on page 143 is used to describe these types of interface flaps and the damping configuration that you can use in each case.

**Figure 6: Two Router Interfaces Connected Through Transport Equipment**

![Diagram of two router interfaces connected through transport equipment.]

**NOTE:** We recommend that you use similar damping configurations on both ends of the physical interface. Configuring damping on one end and not having interface damping on the other end can result in undesired behavior.

The following sections describe the types of interface damping depending upon the transition time length.

- Damping Overview for Shorter Physical Interface Transitions on page 143
- Damping Overview for Longer Physical Interface Transitions on page 144

**Damping Overview for Shorter Physical Interface Transitions**

Figure 6 on page 143 shows two routers with two transport devices between them. If a redundant link between the two transport devices fails, link switching is performed. Link switching takes a number of milliseconds. As shown in Figure 7 on page 144, during switching, both router interfaces might encounter multiple flaps with an up-and-down duration of several milliseconds. These multiple flaps, if advertised to the upper-level routing protocols, might result in undesired route updates. This is why you might want to damp these interface flaps.

**NOTE:** Damping is suitable only with routing protocols.
For shorter physical interface transitions, you configure interface damping with the **hold-time** statement on the interface. The hold timer enables interface damping by not advertising interface transitions until the hold timer duration has passed. When a hold-down timer is configured and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still down, then the router begins to advertise the interface as being down. Similarly, when a hold-up timer is configured and an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still up, then the router begins to advertise the interface as being up.

*Figure 7: Multiple Flaps of Short Duration (Milliseconds)*

---

**Damping Overview for Longer Physical Interface Transitions**

When the link between a router interface and the transport devices is not stable, this can lead to periodic flapping, as shown in *Figure 8 on page 145*. Flaps occur in the order of seconds or more, with an up-and-down flap duration in the order of a second or more. In this case, using the hold timer feature might not produce optimal results as it cannot suppress the relatively longer and repeated interface flaps. Increasing the hold time duration to seconds still allows the system to send route updates on the flapping interface, so fails to suppress periodically flapping interfaces on the system.
For longer periodic interface flaps, you configure interface damping with the `damping` statement on the interface. This damping method uses an exponential back-off algorithm to suppress interface up-and-down event reporting to the upper-level protocols. Every time an interface goes down, a penalty is added to the interface penalty counter. If at some point the accumulated penalty exceeds the suppress level, the interface is placed in the suppress state, and further interface link up and down events are not reported to the upper-level protocols.

**NOTE:**
- Only PTX Series routers, T Series routers, MX960 routers, MX480 routers, MX240 routers, MX80 routers, and M10i routers support interface damping for longer periodic interface flaps on all the line cards.
- Penalty added on every interface flap is 1000.
- The system does not indicate whether an interface is down because of suppression or that is the actual state of the physical interface. Because of this, SNMP link traps and Operation, Administration, and Maintenance (OAM) protocols cannot differentiate the damped version of the link state from the real version. Therefore, the traps and protocols might not work as expected.
- You can verify suppression by viewing the information in the Damping field of the show interface extensive command output.

At all times, the interface penalty counter follows an exponential decay process. Figure 9 on page 147 and Figure 10 on page 148 show the decay process as it applies to recovery when the physical level link is down or up. As soon as the accumulated penalty reaches the lower boundary of the reuse level, the interface is marked as unsuppressed.
and further changes in the interface link state are again reported to the upper-level protocols. You use the `max-suppress` option to configure the maximum time for restricting the accumulation of the penalty beyond the value of the maximum penalty. The value of the maximum penalty is calculated by the software. The maximum penalty corresponds to the time it would take max-suppress to decay and reach the reuse level. The penalty continues to decay after crossing the reuse level.

*Figure 9 on page 147 and Figure 10 on page 148* show the accumulated penalty, and the decay over time as a curve. Whenever the penalty is below the reuse level and the physical level link changes state, state changes are advertised to the system and cause SNMP state changes.

*Figure 9 on page 147* shows the penalty dropping below the reuse level when the physical link is down. The system is notified of a state change only after the physical level link transitions to up.
Figure 9: Physical-Level Link Is Down When the Penalty Falls Below the Reuse Level

Figure 10 on page 148 shows the penalty dropping below the reuse level when the physical link is up. The system is notified of a state change immediately.
Figure 10: Physical-Level Link Is Up When the Penalty Falls Below the Reuse Level

Related Documentation

- Damping Shorter Physical Interface Transitions on page 149
- Damping Longer Physical Interface Transitions on page 150
- Understanding Damping Parameters
- damping on page 498
- hold-time on page 646
### Damping Shorter Physical Interface Transitions

By default, when an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the hardware and Junos OS. In some situations—for example, when an interface is connected to an add/drop multiplexer (ADM) or wavelength-division multiplexer (WDM), or to protect against SONET/SDH framer holes—you might want to damp interface transitions. This means not advertising the interface's transition until a certain period of time has passed, called the **hold-time**. When you have damped interface transitions and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still **down**, then the router begins to advertise the interface as being down. Similarly, when an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still **up**, then the router begins to advertise the interface as being up. For information about physical interface damping, see “Physical Interface Damping Overview” on page 143.

This task applies to damping shorter physical interface transitions in milliseconds. To damp longer physical interface transitions in seconds, see “Damping Longer Physical Interface Transitions” on page 150.

To configure damping of shorter physical interface transitions:

1. Select the interface to damp, where the interface name is `interface-type-fpc/pic/port`:
   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure the hold-time for link up and link down.
   ```
   [edit interfaces interface-name]
   user@host# set hold-time up milliseconds down milliseconds
   ```

   The hold time can be a value from 0 through 4,294,967,295 milliseconds. The default value is 0, which means that interface transitions are not damped. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

   For most Ethernet interfaces, hold timers are implemented using a one-second polling algorithm. For 1-port, 2-port, and 4-port Gigabit Ethernet interfaces with small form-factor pluggable transceivers (SFPs), hold timers are interrupt-driven.

   **NOTE:** The hold-time option is not available for controller interfaces.

---

**Related Documentation**
- Physical Interface Damping Overview on page 143
- Damping Longer Physical Interface Transitions on page 150
Damping Longer Physical Interface Transitions

Physical interface damping limits the advertisement of the up and down transitions (flapping) on an interface. An unstable link between a router interface and the transport devices can lead to periodic flapping. Longer flaps occur with a period of about five seconds or more, with an up-and-down duration of one second. For these longer periodic interface flaps, you configure interface damping with the `damping` statement on the interface. This damping method uses an exponential back-off algorithm to suppress interface up and down event reporting to the upper-level protocols. Every time an interface goes down, a penalty is added to the interface penalty counter. If at some point the accumulated penalty exceeds the suppress level `max-suppress`, the interface is placed in the suppress state, and further interface state up and down transitions are not reported to the upper-level protocols.

**NOTE:**
- Only PTX Series routers, T Series routers, MX2010 routers, MX2020 routers, MX960 routers, MX480 routers, MX240 routers, MX80 routers, and M10i routers support interface damping for longer periodic interface flaps.
- The system does not indicate whether an interface is down because of suppression or that is the actual state of the physical interface. Because of this, SNMP link traps and Operation, Administration, and Maintenance (OAM) protocols cannot differentiate the damped version of the link state from the real version. Therefore, the traps and protocols might not work as expected.
- You can verify suppression by viewing the information in the Damping field of the `show interface extensive` command output.

You can view the damping parameters with the `show interfaces extensive` command.

To configure damping of longer physical interface transitions:

1. Select the interface to damp, where the interface name is `interface-type-fpc/pic/port` or an interface range:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Enable longer interface transition damping on a physical interface:

   ```
   [edit interfaces interface-name damping]
   ```
3. (Optional) Set the maximum time in seconds that an interface can be suppressed no matter how unstable the interface has been.

   NOTE: Configure max-suppress to a value that is greater than the value of half-life; otherwise, the configuration is rejected.

   [edit interfaces interface-name damping]
   user@host# set max-suppress maximum-seconds

4. (Optional) Set the decay half-life in seconds, which is the interval after which the accumulated interface penalty counter is reduced by half if the interface remains stable.

   NOTE: Configure max-suppress to a value that is greater than the value of half-life; otherwise, the configuration is rejected.

   [edit interfaces interface-name damping]
   user@host# set half-life seconds

5. (Optional) Set the reuse threshold (no units). When the accumulated interface penalty counter falls below this value, the interface is no longer suppressed.

   [edit interfaces interface-name damping]
   user@host# set reuse number

6. (Optional) Set the suppression threshold (no units). When the accumulated interface penalty counter exceeds this value, the interface is suppressed.

   [edit interfaces interface-name damping]
   user@host# set suppress number

Related Documentation
- Physical Interface Damping Overview on page 143
- show interfaces extensive on page 1613
- Damping Shorter Physical Interface Transitions on page 149
- damping on page 498
Example: Configuring Physical Interface Damping

This example shows how to configure damping for a physical interface on a PTX Series Packet Transport Router.

• Requirements on page 152
• Overview on page 152
• Configuration on page 153
• Verification on page 153

Requirements

This example uses the following hardware and software components:

• One PTX Series Packet Transport Router
• One or more routers that provide input packets and receive output packets
• Junos OS Release 14.1 or later

Overview

Physical interface damping provides a smoothing of the up and down transitions (flapping) on an interface. Each time a transition occurs, the interface state is changed, which generates an advertisement to the upper-level routing protocols. Damping helps reduce the number of these advertisements.

From the viewpoint of network deployment, physical interface flaps fall into these categories:

• Nearly instantaneous multiple flaps of short duration (milliseconds). For shorter physical interface transitions, you configure interface damping with the **hold-time** statement on the interface. The hold timer enables interface damping by not advertising interface transitions until the hold timer duration has passed. When a hold-down timer is configured and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-down timer period. Similarly, when a hold-up timer is configured and an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-up timer period.

• Periodic flaps of long duration (seconds). For longer periodic interface flaps, you configure interface damping with the **damping** statement on the interface. This damping method uses an exponential back-off algorithm to suppress interface up and down event reporting to the upper-level protocols. Every time an interface goes down, a penalty is added to the interface penalty counter. If at some point the accumulated penalty exceeds the suppress level, the interface is placed in the suppress state, and further interface state up transitions are not reported to the upper-level protocols.
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 interfaces xe-6/0/0 damping half-life 11 max-suppress 2222 reuse 3333 suppress 4444
```

Step-by-Step Procedure

To configure damping on the PTX Series Packet Transport Router:

1. Enable damping on the interface, set the half-life interval, maximum suppression, reuse, and suppress values:

   ```
   [edit interface]
   user@router# set xe-6/0/0 damping half-life 11 max-suppress 2222 reuse 3333 suppress 4444
   ```

2. Commit configuration:

   ```
   [edit]
   user@router# commit
   ```

Results

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

```
user@router# show interfaces
xe-6 {
    damping {
        half-life 11;
        max-suppress 2222;
        reuse 3333;
        suppress 4444;
    }
}
```

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying Interface Damping on xe6 on page 154
Verifying Interface Damping on xe6

**Purpose**

Verify that damping is enabled on the interface and that the damping parameter values are correctly set.

**Action**

From operational mode, run the `show interfaces extensive` command.

```
user@router# run show interfaces xe-6/0/0 extensive
```

Physical interface: xe-6/0/0, Enabled, Physical link is Up
Interface index: 158, SNMP ifIndex: 535, Generation: 161
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error: None, Loopback: None,
Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Damping : half-life: 11 sec, max-suppress: 2222 sec, reuse: 3333, suppress: 4444, state: unsuppressed

**Meaning**

Damping is enabled and configured successfully on the xe-6 interface.

**Related Documentation**

- Physical Interface Damping Overview on page 143
- damping on page 498

Configuring Multiservice Physical Interface Properties

The adaptive services (AS), collector, monitoring services, and monitoring services II interfaces are multiservice interfaces specifically designed to enable IP services. To configure multiservice physical interface properties on the collector, monitoring services, and AS interfaces, include the `multiservice-options` statement:

```
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
    flow-control-options {
      down-on-flow-control;
      dump-on-flow-control;
      reset-on-flow-control;
    }
}
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces cp-fpc/pic/port]`
Enabling or Disabling SNMP Notifications on Physical Interfaces

By default, Simple Network Management Protocol (SNMP) notifications are sent when the state of an interface or a connection changes. You can enable or disable these notification based on your requirements.

To explicitly enable sending SNMP notifications on the physical interface, perform the following steps:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure the `traps` option to enable sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.

   ```
   [edit interfaces interface-name]
   user@host# set traps
   ```

To disable sending SNMP notifications on the physical interface, perform the following steps:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure the `no-traps` option to disable sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.

   ```
   [edit interfaces interface-name]
   user@host# set no-traps
   ```

Related Documentation

- traps on page 1081
**Configuring Accounting for the Physical Interface**

- Accounting Profiles Overview on page 156
- Configuring Accounting for the Physical Interface on page 156
- Displaying Accounting Profile for the Physical Interface on page 157

**Accounting Profiles Overview**

Juniper Networks routers and switches can collect various kinds of data about traffic passing through the router and switch. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router or switch retains before discarding, and the number of bytes per file
- The polling period that the system uses to record the data

You configure the profiles and define a unique name for each profile using statements at the [edit accounting-options] hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the interface-profile statement at the [edit accounting-options] hierarchy level. You configure filter profiles by including the filter-profile statement at the [edit accounting-options] hierarchy level. For more information, see the Network Management and Monitoring Guide.

You apply filter profiles by including the accounting-profile statement at the [edit firewall filter filter-name] and [edit firewall family family filter filter-name] hierarchy levels. For more information, see the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide.

**Configuring Accounting for the Physical Interface**

**Before you begin**

You must configure a profile to collect error and statistic information for input and output packets on a particular physical interface. An accounting profile specifies what statistics should be collected and written to a log file. For more information on how to configure an accounting-data log file, see the Configuring Accounting-Data Log Files.

An interface profile specifies the information collected and written to a log file. You can configure a profile to collect error and statistic information for input and output packets on a particular physical interface.

1. To configure which statistics should be collected for an interface, include the fields statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set fields field-name
2. Each accounting profile logs its statistics to a file in the /var/log directory. To configure which file to use, include the file statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set file filename

   **NOTE:** You must specify a file statement for the interface profile that has already been configured at the [edit accounting-options] hierarchy level. For more information, see the Configuring Accounting-Data Log Files

3. Each interface with an accounting profile enabled has statistics collected once per interval time specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the interval statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set interval minutes

   **NOTE:** The minimum interval allowed is 1 minute. Configuring a low interval in an accounting profile for a large number of interfaces might cause serious performance degradation.

4. To configure the interfaces on which the accounting needs to be performed, apply the interface profile to a physical interface by including the accounting-profile statement at the [edit interfaces interface-name] hierarchy level.

   [edit interfaces]
   user@host# set interface-name accounting-profile profile-name

   **See Also** • Configuring Accounting-Data Log Files

**Displaying Accounting Profile for the Physical Interface**

**Purpose** To display the configured accounting profile a particular physical interface at the [edit accounting-options interface-profile profile-name] hierarchy level:

- interface-name—ge-1/0/1
- Interface profile —if_profile
- File name—if_stats
- Interval—15 minutes
**Action**  
- Run the `show` command at the `[edit edit interfaces ge-1/0/1]` hierarchy level.

```
[edit interfaces ge-1/0/1]
accounting-profile if_profile;
```

- Run the `show` command at the `[edit accounting-options]` hierarchy level.

```
interface-profile if_profile {
  interval 15;
  file if_stats {
    fields {
      input-bytes;
      output-bytes;
      input-packets;
      output-packets;
      input-errors;
      output-errors;
    }
  }
}
```

**Meaning**  
The configured accounting and its associated set options are displayed as expected.

---

**Disabling a Physical Interface**

- Disabling a Physical Interface on page 158
- Example: Disabling a Physical Interface on page 159
- Effect of Disabling Interfaces on T series PICs on page 160

**Disabling a Physical Interface**

You can disable a physical interface, marking it as being down, without removing the interface configuration statements from the configuration.

---

**CAUTION:** Dynamic subscribers and logical interfaces use physical interfaces for connection to the network. The Junos OS allows you to set the interface to disable and commit the change while dynamic subscribers and logical interfaces are still active. This action results in the loss of all subscriber connections on the interface. Use care when disabling interfaces.

---

To disable a physical interface:

1. In configuration mode, go to `[edit interfaces interface-name]` hierarchy level.

```
[edit]
user@host# edit interfaces ge-fpc/pic/port
```

2. Include the `disable` statement.
NOTE: On the router, when you use the disable statement at the edit interfaces hierarchy level, depending on the PIC type, the interface might or might not turn off the laser. Older PIC transceivers do not support turning off the laser, but newer Gigabit Ethernet PICs with SFP and XFP transceivers do support it and the laser will be turned off when the interface is disabled.

WARNING: Do not stare into the laser beam or view it directly with optical instruments even if the interface has been disabled.

Example: Disabling a Physical Interface

Sample interface configuration:

```
[edit interfaces]
user@host# show
ge-0/3/2 {
    unit 0 {
        description CE2-to-PE1;
        family inet {
            address 20.1.1.6/24;
        }
    }
}
```

Disabling the interface:

```
[edit interfaces ge-0/3/2]
user@host# set disable
```

Verifying the interface configuration:

```
[edit interfaces ge-0/3/2]
user@host# show
disable; # Interface is marked as disabled.
unit 0 {
    description CE2-to-PE1;
    family inet {
        address 20.1.1.6/24;
    }
}
```
Effect of Disabling Interfaces on T series PICs

The following table describes the effect of using the `set interfaces disable <interface_name>` statement on T series PICs.

**Table 21: Effect of set interfaces disable <interface_name> on T series PICs**

<table>
<thead>
<tr>
<th>PIC Model Number</th>
<th>PIC Description</th>
<th>Type of PIC</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>PF-12XGE-SFPP</td>
<td>10-Gigabit Ethernet LAN/WAN PIC with SFP+ (T4000 Router)</td>
<td>5</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PF-24XGE-SFPP</td>
<td>10-Gigabit Ethernet LAN/WAN PIC with Oversubscription and SFP+ (T4000 Router)</td>
<td>5</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PF-1CGE-CFP</td>
<td>100-Gigabit Ethernet PIC with CFP (T4000 Router)</td>
<td>5</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PD-4XGE-XFP</td>
<td>10-Gigabit Ethernet, 4-port LAN/WAN XFP</td>
<td>4</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PD-5-10XGE-SFPP</td>
<td>10-Gigabit LAN/WAN with SFP+</td>
<td>4</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PD-1XLE-CFP</td>
<td>40-Gigabit with CFP</td>
<td>4</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PD-1CE-CFP-FPC4</td>
<td>100-Gigabit with CFP</td>
<td>4</td>
<td>Tx laser disabled</td>
</tr>
<tr>
<td>PD-TUNNEL</td>
<td>40-Gigabit Tunnel Services</td>
<td>4</td>
<td>NA</td>
</tr>
<tr>
<td>PD-4OC192-SON-XFP</td>
<td>OC192/STM64, 4-port XFP</td>
<td>4</td>
<td>Tx laser not disabled</td>
</tr>
<tr>
<td>PD-10C768-SON-SR</td>
<td>OC768c/STM256, 1-port</td>
<td>4</td>
<td>Tx laser not disabled</td>
</tr>
</tbody>
</table>

Related Documentation: [disable on page 528]
CHAPTER 3

Configuring Logical Interface Properties

- Logical Interfaces Configuration Properties Overview on page 161
- Logical Interfaces Configuration Statements on page 162
- Logical Interfaces Statements List on page 165
- Specifying the Logical Interface Number on page 172
- Adding a Logical Unit Description to the Configuration on page 172
- Configuring the Interface Bandwidth on page 173
- Configuring Interface Encapsulation on Logical Interfaces on page 173
- Configuring Interface Encapsulation on PTX Series Packet Transport Routers on page 175
- Configuring a Point-to-Point Connection on page 177
- Configuring a Multipoint Connection on page 177
- Configuring the PPP Restart Timers on page 177
- Configuring the PPP Clear Loop Detected Timer on page 178
- Configuring the LCP Configure-Request Maximum Sent on page 178
- Configuring the NCP Configure-Request Maximum Sent on page 179
- Configuring Dynamic Profiles for PPP on page 179
- Configuring PPP CHAP Authentication on page 180
- Configuring the PPP Password Authentication Protocol On a Logical Interface on page 180
- Configuring Accounting for the Logical Interface on page 182
- Enabling or Disabling SNMP Notifications on Logical Interfaces on page 185
- Disabling a Logical Interface on page 185
- Configuring Logical System Interface Properties on page 186

Logical Interfaces Configuration Properties Overview

For a physical interface device to function, you must configure at least one logical interface on that device. For each logical interface, you must specify the protocol family that the interface supports. You can also configure other logical interface properties. These vary by Physical Interface Card (PIC) and encapsulation type, but include the IP address of the interface, and whether the interface supports multicast traffic, data-link connection
identifiers (DLCIs), virtual channel identifiers (VCIs) and virtual path identifiers (VPIs), and traffic shaping.

Related Documentation
- Logical Part of an Interface Name on page 23

Logical Interfaces Configuration Statements

To configure logical interface properties, include the following statements:

```
unit logical-unit-number {
  accept-source-mac {
    mac-address mac-address {
      policer {
        input cos-policer-name;
        output cos-policer-name;
      }
    }
  }
  accounting-profile name;
  allow-any-vci;
  atm-scheduler-map (map-name | default);
  backup-options {
    interface interface-name;
  }
  bandwidth rate;
  cell-bundle-size cells;
  clear-dont-fragment-bit;
  compression {
    rtp {
      f-max-period number;
      queues [ queue-numbers ];
      port {
        minimum port-number;
        maximum port-number;
      }
    }
  }
  compression-device interface-name;
  copy-tos-to-outer-ip-header;
  demux-destination family;
  demux-source family;
  demux-options {
    underlying-interface interface-name;
  }
  description text;
  interface {
    l2tp-interface-id name:
    (dedicated | shared);
  }
  dialer-options {
    activation-delay seconds;
    callback;
  }
```
callback-wait-period time;
deactivation-delay seconds;
dial-string [ dial-string-numbers ];
idle-timeout seconds;
incoming-map {
caller (caller-id] accept-all);
initial-route-check seconds;
load-interval seconds;
load-threshold number;
pool pool-name;
redial-delay time;
watch-list [
[ routes ];
}
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold ppp1 cells;
filter filter-name;
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
  inner-tag-protocol-id;
  inner-vlan-id;
  [ (pop | pop-pop | pop-swap | push | push-push | swap [swap-push | swap-swap];
tag-protocol-id tpid;
  vlan-id number;
}
interleave-fragments;
inverse-arp;
link-layer-overhead percent;
layer2-policer {
  input-policer policer-name;
  input-three-color policer-name;
  output-policer policer-name;
  output-three-color policer-name;
}
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
  up-count cells;
  down-count cells;
}
oam-period (seconds | disable);
output-vlan-map {
  inner-tag-protocol-id;
  inner-vlan-id;
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  tag-protocol-id tpid;
  vlan-id number;
}

passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
  chap {
    access-profile name;
    default-chap-secret name;
    local-name name;
    passive;
  }
  compression {
    acfc;
    pfc;
  }
  dynamic-profile profile-name;
lcp-restart-timer milliseconds;
loopback-clear-timer seconds;
ncp-restart-timer milliseconds;
pap {
  default-pap-password password;
  local-name name;
  local-password password;
  passive;
}
pppoe-options {
  access-concentrator name;
  auto-reconnect seconds;
  (client | server);
  service-name name;
  underlying-interface interface-name;
}
proxy-arp;
service-domain (inside | outside);
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}
short-sequence;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
  backup-destination address;
  destination address;
You can include these statements at the following hierarchy levels:

- [edit interfaces interface-name]
- [edit logical-systems logical-system-name interfaces interface-name]

For information about interface-specific logical properties, see Table 22 on page 165.

**Logical Interfaces Statements List**

Table 22 on page 165 lists statements that you can use to configure logical interfaces.

**Table 22: Statements for Logical Interface Properties**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-profile name</td>
<td>ATM2 IQ interfaces</td>
<td>“Configuring the PPP Password Authentication Protocol On a Logical Interface” on page 180</td>
</tr>
<tr>
<td>accept-source-mac</td>
<td>Gigabit Ethernet intelligent queuing (IQ) interfaces</td>
<td>Configuring MAC Address Filtering</td>
</tr>
<tr>
<td>accounting-profile name</td>
<td>All</td>
<td>“Configuring Accounting for the Logical Interface” on page 182</td>
</tr>
<tr>
<td>allow-any-vci</td>
<td>Asynchronous Transfer Mode (ATM) interfaces</td>
<td>Configuring ATM Interface Encapsulation</td>
</tr>
<tr>
<td>atm-scheduler-map (map-name</td>
<td>default)</td>
<td>ATM2 IQ interfaces</td>
</tr>
<tr>
<td>backup-destination address</td>
<td>Encryption interfaces</td>
<td>Class of Service Feature Guide (Routers and EX9200 Switches)</td>
</tr>
</tbody>
</table>
Table 22: Statements for Logical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bandwidth rate</strong></td>
<td>All interfaces, except multilink and aggregated</td>
<td>“Configuring the Interface Bandwidth” on page 173</td>
</tr>
<tr>
<td><strong>cbr rate</strong></td>
<td>ATM interfaces</td>
<td>Defining the ATM Traffic-Shaping Profile Overview</td>
</tr>
<tr>
<td><strong>cell-bundle-size cells</strong></td>
<td>ATM2 IQ interfaces</td>
<td>Configuring the Layer 2 Circuit Cell-Relay Cell Maximum Overview</td>
</tr>
<tr>
<td><strong>clear-dont-fragment-bit</strong></td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>compression</strong></td>
<td>AS PIC or MultiServices PIC link services IQ interfaces (lsq) and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>copy-tos-to-outer-ip-header</strong></td>
<td>GRE tunnel interfaces</td>
<td>Class of Service Feature Guide (Routers and EX9200 Switches)</td>
</tr>
<tr>
<td><strong>demux-destination family</strong></td>
<td>IP demux interfaces</td>
<td>“Configuring an IP Demultiplexing Interface” on page 296</td>
</tr>
<tr>
<td><strong>demux-options family</strong></td>
<td>IP demux interfaces</td>
<td>“Configuring an IP Demultiplexing Interface” on page 296</td>
</tr>
<tr>
<td><strong>demux-source family</strong></td>
<td>IP demux interfaces</td>
<td>“Configuring an IP Demultiplexing Interface” on page 296</td>
</tr>
<tr>
<td><strong>description text</strong></td>
<td>All</td>
<td>“Adding a Logical Unit Description to the Configuration” on page 172</td>
</tr>
<tr>
<td>**destination (address</td>
<td>routing-instance-name)</td>
<td>Encryption generic routing encapsulation (GRE) tunnel, and IP tunnel interfaces</td>
</tr>
<tr>
<td><strong>disable</strong></td>
<td>All</td>
<td>“Disabling a Logical Interface” on page 185</td>
</tr>
<tr>
<td><strong>disable-mlppp-inner-ppp-pfc</strong></td>
<td>MLPPP interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>dlci dlci-identifier</strong></td>
<td>Point-to-point interfaces with Frame Relay encapsulation</td>
<td>Configuring Frame Relay DLCIs</td>
</tr>
<tr>
<td><strong>drop-timeout milliseconds</strong></td>
<td>Multilink interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>dynamic-profile profile-name</strong></td>
<td>1-Gigabit Ethernet and 10-Gigabit Ethernet interfaces configured with PPP over Ethernet on M120 and M320 routers</td>
<td>Junos Subscriber Access Configuration Guide</td>
</tr>
</tbody>
</table>
### Table 22: Statements for Logical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>encapsulation type</strong></td>
<td>All interfaces, except aggregated SONET/SDH and loopback</td>
<td>Configuring Interface Encapsulation on Logical Interfaces</td>
</tr>
<tr>
<td><strong>epd-threshold cells</strong></td>
<td>ATM2 IQ interfaces</td>
<td>Configuring the ATM2 IQ EPD Threshold</td>
</tr>
<tr>
<td><strong>f-max-period number</strong></td>
<td>AS PIC or MultiServices link services IQ interfaces (lsq-) and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>family</strong></td>
<td>All</td>
<td>“Configuring the Protocol Family” on page 190</td>
</tr>
<tr>
<td><strong>fragment-threshold bytes</strong></td>
<td>Multilink interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>inner-tag-protocol-id</strong></td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>802.1Q VLANs Overview</td>
</tr>
<tr>
<td><strong>inner-vlan-id</strong></td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>802.1Q VLANs Overview</td>
</tr>
<tr>
<td><strong>inner-vlan-id-range</strong></td>
<td>Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet IQ interfaces</td>
<td>“Configuring ATM-to-Ethernet Interworking” on page 262</td>
</tr>
<tr>
<td><strong>input</strong></td>
<td>AS PIC or MultiServices link services</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>input-policer policer-name</strong></td>
<td>For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series and T Series routers</td>
<td>Junos OS Services Interfaces Library for Routing Devices and Configuring Gigabit Ethernet Two-Color and Tricolor Policers</td>
</tr>
<tr>
<td><strong>input-three-color policer-name</strong></td>
<td>For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series and T Series routers</td>
<td>Class of Service Feature Guide (Routers and EX9200 Switches) and Configuring Gigabit Ethernet Two-Color and Tricolor Policers</td>
</tr>
<tr>
<td><strong>input-vlan-map</strong></td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview</td>
</tr>
<tr>
<td><strong>interleave-fragments</strong></td>
<td>Link services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>inverse-arp</strong></td>
<td>Interfaces with ATM and Frame Relay encapsulation</td>
<td>Configuring Inverse ATM1 or ATM2 ARP and Configuring Inverse Frame Relay ARP</td>
</tr>
<tr>
<td><strong>key number</strong></td>
<td>GRE tunnel interfaces on Adaptive Services PICs</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td><strong>layer2-policer</strong></td>
<td>1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces</td>
<td>Configuring Gigabit Ethernet Two-Color and Tricolor Policers</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lcp-restart-timer</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Restart Timers” on page 177</td>
</tr>
<tr>
<td>l2tp-interface-id <strong>name</strong></td>
<td>Adaptive services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>link-layer-overhead <strong>percent</strong></td>
<td>AS PIC or MultiServices link services IQ interfaces (lsq)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>local-name <strong>name</strong></td>
<td>ATM2 IQ interfaces</td>
<td>“Configuring PPP CHAP Authentication” on page 180 and “Configuring the PPP Password Authentication Protocol On a Logical Interface” on page 180</td>
</tr>
<tr>
<td>mac-address <strong>mac-address</strong></td>
<td>Gigabit Ethernet interfaces and Gigabit Ethernet IQ and IQE interfaces with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring MAC Address Filtering</td>
</tr>
<tr>
<td>minimum-links <strong>number</strong></td>
<td>Multilink interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>mrru <strong>bytes</strong></td>
<td>Multilink interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>multicast-dlci <strong>dli-identifier</strong></td>
<td>Point-to-multipoint Frame Relay interfaces</td>
<td>Configuring a Multicast–Capable Frame Relay Connection</td>
</tr>
<tr>
<td>multicast-vci <strong>vid-identifier</strong></td>
<td>Point-to-multipoint ATMI and ATM2 IQ interfaces</td>
<td>Configuring the ATM OAM F5 Loopback Cell Threshold</td>
</tr>
<tr>
<td>multilink-max-classes <strong>number</strong></td>
<td>AS PIC or MultiServices link services IQ interfaces (lsq-)</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>multipoint</td>
<td>All</td>
<td>“Configuring a Multipoint Connection” on page 177</td>
</tr>
<tr>
<td>ncp-restart-timer</td>
<td>Interfaces with PPP encapsulation</td>
<td>“Configuring the PPP Restart Timers” on page 177</td>
</tr>
<tr>
<td>oam-liveness</td>
<td>ATMI and ATM2 IQ interfaces</td>
<td>Configuring the ATM OAM F5 Loopback Cell Threshold</td>
</tr>
<tr>
<td>oam-period (disable</td>
<td>seconds)</td>
<td>ATMI and ATM2 IQ interfaces</td>
</tr>
<tr>
<td>Statement</td>
<td>Interface Types</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>output</td>
<td>All</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>output-policer</td>
<td>For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series and T Series routers</td>
<td>Class of Service Feature Guide (Routers and EX9200 Switches) and Configuring Gigabit Ethernet Two-Color and Tricolor Policers</td>
</tr>
<tr>
<td>output-three-color</td>
<td>For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series and T Series routers</td>
<td>Class of Service Feature Guide (Routers and EX9200 Switches) and Configuring Gigabit Ethernet Two-Color and Tricolor Policers</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview</td>
</tr>
<tr>
<td>passive (CHAP)</td>
<td>ATM2 IQ interfaces</td>
<td>&quot;Configuring PPP CHAP Authentication&quot; on page 180</td>
</tr>
<tr>
<td>passive (PAP)</td>
<td>ATM2 IQ interfaces</td>
<td>&quot;Configuring the PPP Password Authentication Protocol On a Logical Interface&quot; on page 180</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>SONET/SDH interfaces</td>
<td>Enabling Packet Flow Monitoring on SONET/SDH Interfaces</td>
</tr>
<tr>
<td>peer-unit unit-number</td>
<td>Logical tunnel interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>pfc</td>
<td>Interfaces with PPP, PPP CCC, or PPP TCC encapsulation</td>
<td>&quot;Configuring the PPP Protocol Field Compression&quot; on page 135</td>
</tr>
<tr>
<td>plp1 cells</td>
<td>ATM2 IQ interfaces</td>
<td>Configuring the ATM2 IQ EPD Threshold</td>
</tr>
<tr>
<td>plp-to-clp</td>
<td>ATM2 IQ interfaces</td>
<td>Enabling the PLP Setting to Be Copied to the CLP Bit</td>
</tr>
<tr>
<td>point-to-point</td>
<td>All</td>
<td>&quot;Configuring a Point-to-Point Connection&quot; on page 177</td>
</tr>
<tr>
<td>policer</td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router)</td>
<td>Configuring MAC Address Filtering</td>
</tr>
<tr>
<td>pop</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Removing a VLAN Tag</td>
</tr>
<tr>
<td>pop-pop</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Removing the Outer and Inner VLAN Tags</td>
</tr>
<tr>
<td>pop-swap</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag</td>
</tr>
</tbody>
</table>
Table 22: Statements for Logical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>AS PIC or MultiServices or MultiServices link services IQ interfaces (lsq) and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>ppp-options</td>
<td>Interfaces with PPP, PPP CCC, or PPP TCC encapsulation</td>
<td>“Configuring PPP CHAP Authentication” on page 180 and “Configuring the PPP Password Authentication Protocol On a Logical Interface” on page 180</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>Ethernet interfaces</td>
<td>Configuring Restricted and Unrestricted Proxy ARP</td>
</tr>
<tr>
<td>push</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Stacking a VLAN Tag</td>
</tr>
<tr>
<td>push-push</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Stacking Two VLAN Tags</td>
</tr>
<tr>
<td>queue-length number</td>
<td>ATMI interfaces</td>
<td>Configuring the ATMI Queue Length</td>
</tr>
<tr>
<td>queues [queue-numbers]</td>
<td>AS PIC or MultiServices link services IQ interfaces (lsq) and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>routing-instance</td>
<td>GRE tunnel and IP tunnel interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>rtp</td>
<td>AS PIC or MultiServices link services IQ interfaces (lsq) and voice services interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>rtvbr peak rate sustained rate burst length</td>
<td>ATM2 interfaces</td>
<td>Configuring ATM CBR</td>
</tr>
<tr>
<td>service-domain (inside</td>
<td>outside)</td>
<td>Adaptive services interfaces</td>
</tr>
<tr>
<td>shaping</td>
<td>ATMI and ATM2 IQ interfaces</td>
<td>Defining the ATM Traffic-Shaping Profile Overview</td>
</tr>
<tr>
<td>short-sequence</td>
<td>Multilink interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>source source-address</td>
<td>Encryption, GRE tunnel, and IP tunnel interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>swap</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames</td>
</tr>
<tr>
<td>swap-push</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Rewriting a VLAN Tag and Adding a New Tag</td>
</tr>
</tbody>
</table>
Table 22: Statements for Logical Interface Properties (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Interface Types</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap-swap</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Rewriting the Inner and Outer VLAN Tags</td>
</tr>
<tr>
<td>tag-protocol-id tpid</td>
<td>Gigabit Ethernet and Gigabit Ethernet IQ and IQE PICs with SFPs (except the</td>
<td>Rewriting the VLAN Tag on Tagged Frames</td>
</tr>
<tr>
<td></td>
<td>10-port Gigabit Ethernet PIC, Aggregated Ethernet with Gigabit Ethernet IQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interfaces, and the built-in Gigabit Ethernet port on the M7i router)</td>
<td></td>
</tr>
<tr>
<td>transmit-weight number</td>
<td>ATM2 IQ interfaces</td>
<td>Configuring the ATM2 IQ Transmission Weight</td>
</tr>
<tr>
<td>(traps</td>
<td>no-traps)</td>
<td>All</td>
</tr>
<tr>
<td>trunk-bandwidth rate</td>
<td>ATM2 IQ interfaces</td>
<td>Configuring Layer 2 Circuit Trunk Mode Scheduling Overview</td>
</tr>
<tr>
<td>trunk-id number</td>
<td>ATM2 IQ interfaces</td>
<td>Configuring Layer 2 Circuit Transport Mode</td>
</tr>
<tr>
<td>ttl number</td>
<td>GRE tunnel and IP tunnel interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>tunnel</td>
<td>Encryption, GRE tunnel, and IP tunnel interfaces</td>
<td>Junos OS Services Interfaces Library for Routing Devices</td>
</tr>
<tr>
<td>underlying-interface</td>
<td>IP demux interfaces</td>
<td>“Configuring an IP Demultiplexing Interface” on page 296</td>
</tr>
<tr>
<td>vbr peak rate sustained rate burst length</td>
<td>ATM interfaces</td>
<td>Defining the ATM Traffic-Shaping Profile Overview</td>
</tr>
<tr>
<td>vci vpi-identifiervci-identifier</td>
<td>ATM1 and ATM2 IQ point-to-point interfaces</td>
<td>Configuring a Point-to-Point ATM1 or ATM2 IQ Connection</td>
</tr>
<tr>
<td>vci-range</td>
<td>ATM2 IQ interfaces</td>
<td>“Configuring ATM-to-Ethernet Interworking” on page 262</td>
</tr>
<tr>
<td>vpi vpi-identifier</td>
<td>ATM1 and ATM2 IQ point-to-point interfaces</td>
<td>Configuring a Point-to-Point ATM1 or ATM2 IQ Connection</td>
</tr>
<tr>
<td>vlan-id number</td>
<td>Fast Ethernet, Gigabit Ethernet, and Gigabit Ethernet IQ interfaces and</td>
<td>Binding VLAN IDs to Logical Interfaces and Rewriting the VLAN Tag on Tagged</td>
</tr>
<tr>
<td></td>
<td>aggregated Ethernet using Gigabit Ethernet IQ interfaces</td>
<td>Frames</td>
</tr>
<tr>
<td>vlan-tags inner tpidvlan-id</td>
<td>Gigabit Ethernet IQ interfaces</td>
<td>Configuring Dual VLAN Tags</td>
</tr>
<tr>
<td>outer tpidvlan-id</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
Specifying the Logical Interface Number

Each logical interface must have a logical unit number. The logical unit number corresponds to the logical unit part of the interface name. For more information, see “Interface Naming Overview” on page 16.

Point-to-Point Protocol (PPP), Cisco High-level Data Link Control (HDLC), and Ethernet circuit cross-connect (CCC) encapsulations support only a single logical interface, whose logical unit number must be 0. Frame Relay and ATM encapsulations support multiple logical interfaces, so you can configure one or more logical unit numbers.

You specify the logical unit number by including the unit statement:

```
unit logical-unit-number {
  ...
}
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name ]`
- `[edit logical-systems logical-system-name interfaces interface-name ]`

The range of number available for the logical unit number varies for different interface types. See unit for current range values.

Adding a Logical Unit Description to the Configuration

You can include a text description of each logical unit in the configuration file. Any descriptive text you include is displayed in the output of the show interfaces commands, and is also exposed in the ifAlias Management Information Base (MIB) object. It has no impact on the interface’s configuration. To add a text description, include the description statement:

```
description text;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number ]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ]`

The description can be a single line of text. If the text contains spaces, enclose it in quotation marks.

---

**NOTE:** You can configure the extended DHCP relay to include the interface description in the option 82 Agent Circuit ID suboption. See “Using DHCP Relay Agent Option 82 Information” in the Junos OS Broadband Subscriber Management and Services Library.
For information about describing physical interfaces, see “Configuring Interface Description” on page 98.

Configuring the Interface Bandwidth

By default, the Junos OS uses the physical interface’s speed for the MIB-II object, ifSpeed. You can configure the logical unit to populate the ifSpeed variable by configuring a bandwidth value for the logical interface. The bandwidth statement sets an informational-only parameter; you cannot adjust the actual bandwidth of an interface with this statement.

NOTE: We recommend that you be careful when setting this value. Any interface bandwidth value that you configure using the bandwidth statement affects how the interface cost is calculated for a dynamic routing protocol, such as OSPF. By default, the interface cost for a dynamic routing protocol is calculated using the following formula:

\[
\text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}},
\]

where bandwidth is the physical interface speed. However, if you specify a value for bandwidth using the bandwidth statement, that value is used to calculate the interface cost, rather than the actual physical interface bandwidth.

To configure the bandwidth value for a logical interface, include the bandwidth statement:

```
bandwidth rate;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

rate is the peak rate, in bps or cps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps. The value can be any positive integer. The bandwidth statement is valid for all logical interfaces, except multilink interfaces.

Configuring Interface Encapsulation on Logical Interfaces

- Understanding Interface Encapsulation on Logical Interfaces on page 174
- Configuring the Encapsulation on a Logical Interface on page 174
- Displaying the Encapsulation on a Logical Interface on page 175
Understanding Interface Encapsulation on Logical Interfaces

You can configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

The following restrictions apply to logical interface encapsulation:

- With the atm-nlpid, atm-cisco-nlpid, and atm-vc-mux encapsulations, you can configure the inet family only.
- With the CCC circuit encapsulations, you cannot configure a family on the logical interface.
- A logical interface cannot have frame-relay-ccc encapsulation unless the physical device also has frame-relay-ccc encapsulation.
- A logical interface cannot have frame-relay-tcc encapsulation unless the physical device also has frame-relay-tcc encapsulation. In addition, you must assign this logical interface a DLCI from 512 through 1022 and configure it as point-to-point.
- A logical interface cannot have frame-relay-ether-type or frame-relay-ether-type-tcc encapsulation unless the physical interface has flexible-frame-relay encapsulation and is on an IQ or IQE PIC.
- For frame-relay-ether-type-tcc encapsulation, you must assign this logical interface a DLCI from 512 through 1022.
- For interfaces that carry IP version 6 (IPv6) traffic, you cannot configure ether-over-atm-llc encapsulation.
- When you use ether-over-atm-llc encapsulation, you cannot configure multipoint interfaces.
- A logical interface cannot have vlan-ccc or vlan-vpls encapsulation unless the physical device also has vlan-ccc or vlan-vpls encapsulation, respectively. In addition, you must assign this logical interface a VLAN ID from 512 through 1023; if the VLAN ID is 511 or lower, it is subject to the normal destination filter lookups in addition to source address filtering. For more information, see Configuring VLAN and Extended VLAN Encapsulation.
- You can create an ATM cell-relay circuit by configuring an entire ATM physical device or an individual virtual circuit (VC). When you configure an entire device, only cell-relay encapsulation is allowed on the logical interfaces. For more information, see Configuring an ATM Cell-Relay Circuit Overview.

Configuring the Encapsulation on a Logical Interface

Generally, you configure an interface’s encapsulation at the [edit interfaces interface-name] hierarchy level. However, for some encapsulation types, such as Frame Relay, ATM, and Ethernet virtual local area network (VLAN) encapsulations, you can also configure the encapsulation type that is used inside the Frame Relay, ATM, or VLAN circuit itself.
To configure encapsulation on a logical interface:

1. In configuration mode, go to the [edit interfaces interface-name unit logical-unit-number] or [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number] hierarchy level.

   [edit]
   user@host# set interfaces at-fpc/pic/port unit logical-unit-number

2. Configure the encapsulation type as described in encapsulation (Logical Interface).

   [edit interfaces at-fpc/pic/port unit logical-unit-number]
   user@host# set encapsulation encapsulation-type

Displaying the Encapsulation on a Logical Interface

<table>
<thead>
<tr>
<th>Purpose</th>
<th>To display the configured encapsulation and its associated set options on a physical interface when the following are set at the [edit interfaces interface-name] or [edit logical-systems logical-system-name interfaces interface-name] hierarchy level:</th>
</tr>
</thead>
</table>
|                  | • interface-name—at-1/1/0  
|                  | • Encapsulation—atm-ccc-cell-relay  
|                  | • Unit—120  |

<table>
<thead>
<tr>
<th>Action</th>
<th>Run the show command at the [edit interfaces interface-name] hierarchy level.</th>
</tr>
</thead>
</table>
|                  | [edit interfaces at-1/1/0]  
|                  | user@host# show  
|                  | encapsulation atm-ccc-cell-relay;  
|                  | unit 120 {  
|                  |   encapsulation atm-ccc-cell-relay;  
|                  | }  |

| Meaning          | The configured encapsulation and its associated set options are displayed as expected. |

<table>
<thead>
<tr>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation (Logical Interface) on page 567</td>
</tr>
<tr>
<td>Configuring VLAN and Extended VLAN Encapsulation</td>
</tr>
<tr>
<td>Configuring an ATMI Cell-Relay Circuit Overview</td>
</tr>
</tbody>
</table>

Configuring Interface Encapsulation on PTX Series Packet Transport Routers

This topic describes how to configure interface encapsulation on PTX Series Packet Transport Routers. Use the flexible-ethernet-services configuration statement to configure different encapsulation for different logical interfaces under a physical interface. With
flexible Ethernet services encapsulation, you can configure each logical interface encapsulation without range restrictions for VLAN IDs.

Supported encapsulations for physical interfaces include:

- **flexible-ethernet-services**
- **ethernet-ccc**
- **ethernet-tcc**

Supported encapsulations for logical interfaces include:

- **ethernet**
- **vlan-ccc**
- **vlan-tcc**

**NOTE:** PTX Series Packet Transport Routers do not support extended-vlan-ccc and extended-vlan-tcc encapsulation on logical interfaces. Instead, you can configure a tag protocol ID (TPID) value of 0x9100 to achieve the same results.

To configure flexible Ethernet services encapsulation, include the `encapsulation flexible-ethernet-services` statement at the `[edit interfaces et-fpc/.pic/port ]` hierarchy level. For example:

```plaintext
interfaces {
    et-fpc/.pic/port {
        vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 0 {
            vlan-id 1000;
            family inet {
                address 11.0.0.20/24;
            }
        }
        unit 1 {
            encapsulation vlan-ccc;
            vlan-id 1010;
        }
        unit 2 {
            encapsulation vlan-tcc;
            vlan-id 1020;
            family tcc {
                proxy {
                    inet-address 11.0.2.160;
                }
                remote {
                    inet-address 11.0.2.10;
                }
            }
        }
    }
}
```
By default, all interfaces are assumed to be point-to-point connections. You must ensure that the maximum transmission unit (MTU) sizes on both sides of the connection are the same.

For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, you can explicitly configure an interface to be a point-to-point connection by including the `point-to-point` statement:

```
point-to-point;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

### Configuring a Multipoint Connection

By default, all interfaces are assumed to be point-to-point connections. To configure an interface to be a multipoint connection, include the `multipoint` statement:

```
multipoint;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

### Configuring the PPP Restart Timers

You can configure a restart timer for the Link Control Protocol (LCP) and Network Control Protocol (NCP) components of a PPP session. You can configure the LCP restart timer on interfaces with PPP, PPP TCC, PPP over Ethernet, PPP over ATM, and PPP over Frame Relay encapsulations. You can configure the NCP restart timer on interfaces with PPP and PPP TCC encapsulations and on multilink PPP bundle interfaces.

To configure the restart timer for the NCP component of a PPP session, include the `ncp-restart-timer` statement, and specify the number of milliseconds.
To configure the restart timer for the LCP component of a PPP session, include the `lcp-restart-timer` statement, and specify the number of milliseconds:

```
lcp-restart-timer milliseconds;
ncp-restart-timer milliseconds;
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number ppp-options]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]`

To monitor the configuration, issue the `show interfaces interface-name` command. Configured options are displayed in the `PPP parameters` field for the physical interface.

```
user@host> run show interfaces t1-0/0/0:1:1.0 detail

Logical interface t1-0/0/0:1:1.0 (Index 67) (SNMP ifIndex 40)
(Generation 156)
  Flags: Hardware-Down Device-Down Point-To-Point SNMP-Traps 0x4000
  Encapsulation: PPP
  PPP parameters:
    LCP restart timer: 2000 msec
    NCP restart timer: 2000 msec
  Protocol inet, MTU: 1500, Generation: 163, Route table: 0
  Flags: Protocol-Down
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 1.1.1/24, Local: 1.1.1.2, Broadcast: 1.1.1.255
```

Configuring the PPP Clear Loop Detected Timer

When a Point-to-Point Protocol (PPP) session detects a loop, the loop detected flag is set. If the flag is not cleared by the protocol after the loopback is cleared, the clear loop detected timer clears the flag after the specified time has elapsed.

To configure the clear loop detected timer for the LCP component of a PPP session, include the `loopback-clear-timer` statement, and specify the number of seconds.

```
loopback-clear-timer seconds;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number ppp-options]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]`

To monitor the configuration, issue the `show interfaces interface-name extensive` command.

Configuring the LCP Configure-Request Maximum Sent

Link Control Protocol (LCP) Configure-Request is used to establish a link. You can configure the maximum number of LCP Configure-Requests to send. The router stops
sending LCP Configure-Requests after the specified maximum number is sent. To configure the LCP Configure-Request maximum, use the `lcp-max-conf-req` statement at the `[edit interfaces interface-name unit number ppp-options]` hierarchy level. The `number` range is from 0 to 65,535; where 0 specifies no limit and the LCP Configure-Request is sent indefinitely. The default is 254.

### Related Documentation
- `lcp-max-conf-req` on page 727

#### Configuring the NCP Configure-Request Maximum Sent

Network Control Protocol (NCP) Configure-Request is used to establish a link. You can configure the maximum number of NCP Configure-Requests to send. The router stops sending NCP Configure-Requests after the specified maximum number is sent. To configure the NCP Configure-Request maximum, use the `ncp-max-conf-req` statement at the `[edit interfaces interface-name unit number ppp-options]` hierarchy level. The `number` range is from 0 to 65,535; where 0 specifies no limit and NCP Configure-Request is sent indefinitely. The default is 254.

### Related Documentation
- `ncp-max-conf-req` on page 727

#### Configuring Dynamic Profiles for PPP

A dynamic profile acts as a template that enables you to create, update, or remove a configuration that includes attributes for client access (for example, interface or protocol) or service (for example, IGMP). Using these profiles you can consolidate all of the common attributes of a client (and eventually a group of clients) and apply the attributes simultaneously.

After they are created, the profiles reside in a profile library on the router. You can then use the `dynamic-profile` statement to attach profiles to interfaces. To assign a dynamic profile to a PPP interface, you can include the `dynamic-profile` statement at the `[edit interfaces interface-name unit logical-unit-number ppp-options]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number ppp-options]
dynamic-profile profile-name;
```

To monitor the configuration, issue the `show interfaces interface-name` command.

For information about dynamic profiles, see `Dynamic Profiles Overview` in the *Junos Subscriber Access Configuration Guide*.

For information about creating dynamic profiles, see `Configuring a Basic Dynamic Profile` in the *Junos Subscriber Access Configuration Guide*.

For information about assigning a dynamic profile to a PPP interface, see `Attaching Dynamic Profiles to Static PPP Subscriber Interfaces` in the *Junos Subscriber Access Configuration Guide*.
For information about using dynamic profiles to authenticate PPP subscribers, see *Configuring Dynamic Authentication for PPP Subscribers*.

**NOTE:** Dynamic profiles for PPP subscribers are supported only on PPPoE interfaces for this release.

### Configuring PPP CHAP Authentication

For interfaces with PPP encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP), as defined in RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*. When you enable CHAP on an interface, the interface can authenticate its peer and can be authenticated by its peer.

For information about configuring CHAP, see “Configuring the PPP Challenge Handshake Authentication Protocol” on page 121.

### Configuring the PPP Password Authentication Protocol On a Logical Interface

- Understanding PPP Password Authentication Protocol on page 180
- Configuring the PPP Password Authentication Protocol On a Logical Interface on page 181

### Understanding PPP Password Authentication Protocol

The Password Authentication Protocol (PAP) provides a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment.

After the link is established, an ID and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

For interfaces with PPP encapsulation, you can configure interfaces to support the Password Authentication Protocol (PAP), as defined in RFC 1334, *PAP Authentication Protocols*. If authentication is configured, the PPP link negotiates using CHAP or PAP protocol for authentication during the Link Control Protocol (LCP) negotiation phase. PAP is only performed after the link establishment phase (LCP up) portion of the authentication phase.

During authentication, the PPP link sends a PAP authentication-request packet to the peer with an ID and password. The authentication-request packet is sent every 2 seconds, similar to the CHAP challenge, until a response is received (acknowledgment packet, nonacknowledgment packet). If an acknowledgment packet is received, the PPP link transitions to the next state, the network phase. If a nonacknowledgment packet is received, an LCP terminate request is sent, and the PPP link goes back to the link establishment phase. If no response is received, and an optional retry counter is set to **true**, a new request acknowledgment packet is resent. If the retry counter expires, the PPP link transitions to the LCP negotiate phrase.
You can configure the PPP link with PAP in passive mode. By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation—in passive mode, the interface does not authenticate the peer.

**Configuring the PPP Password Authentication Protocol On a Logical Interface**

When you configure an interface to use PAP, you must assign an access profile to the interface. When an interface receives PAP authentication requests, the access profile in the packet is used to look up the password. If no matching access profile is found for the PAP authentication request that was received by the interface, the optionally configured default PAP password is used.

To configure the PPP password authentication protocol, on each logical interface with PPP encapsulation, perform the following steps.

1. The default PAP password is used when no matching PAP access profile exists, or if the PAP access profile name changes during PPP link negotiation. To configure the default PAP password, include the `pap-password` statement at the `[edit interfaces interface-name unit logical-unit-number ppp-options pap]` hierarchy level:

   ```
   user@host# set default-pap-password password
   ```

2. To configure the name the interface uses in PAP request and response packets, include the `local-name` statement at the `[edit interfaces interface-name unit logical-unit-number ppp-options pap]` hierarchy level:

   ```
   user@host# set local-name name
   ```

   **NOTE:** By default, when PAP is enabled on an interface, the interface uses the router’s system hostname as the name sent in PAP request and response packets.

3. You need to configure the password to be used for authentication. To configure the host password for sending PAP requests, include the `local-password` statement at the `[edit interfaces interface-name unit logical-unit-number ppp-options pap]` hierarchy level:

   ```
   user@host# set local-password password
   ```
4. To configure the interface to authenticate with PAP in passive mode, include the `passive` statement at the `[edit interfaces interface-name unit logical-unt-number ppp-options pap]` hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unt-number ppp-options pap]
user@host# set passive
```

**NOTE:** By default, when PAP is enabled on an interface, the interface expects authenticate-request packets from the peer. However, the interface can be configured to send authentication request packets to the peer by configuring PAP to operate in passive mode. In PAP passive mode, the interface sends the authenticate-request packets to the peer only if the interface receives the PAP option from the peer during LCP negotiation—in passive mode, the interface does not authenticate the peer.

**See Also**  
*Configuring the PPP Authentication Protocol*

### Configuring Accounting for the Logical Interface

- Accounting Profiles Overview on page 182
- Configuring Accounting for the Logical Interface on page 183
- Displaying Accounting Profile for the Logical Interface on page 184

#### Accounting Profiles Overview

Juniper Networks routers and switches can collect various kinds of data about traffic passing through the router and switch. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router or switch retains before discarding, and the number of bytes per file
- The polling period that the system uses to record the data

You configure the profiles and define a unique name for each profile using statements at the `[edit accounting-options]` hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the `interface-profile` statement at the `[edit accounting-options]` hierarchy level. You configure filter profiles by including the `filter-profile` statement at the `[edit accounting-options]` hierarchy level. For more information, see the Network Management and Monitoring Guide.

You apply filter profiles by including the `accounting-profile` statement at the `[edit firewall filter filter-name]` and `[edit firewall family family filter filter-name]` hierarchy levels. For more information, see the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide.
Configuring Accounting for the Logical Interface

Before you begin

You must configure a profile to collect error and statistic information for input and output packets on a particular logical interface. An accounting profile specifies what statistics should be collected and written to a log file. For more information on how to configure an accounting-data log file, see the Configuring Accounting-Data Log Files.

An interface profile specifies the information collected and written to a log file. You can configure a profile to collect error and statistic information for input and output packets on a particular logical interface.

1. To configure which statistics should be collected for an interface, include the fields statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set fields field-name

2. Each accounting profile logs its statistics to a file in the /var/log directory. To configure which file to use, include the file statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set file filename

   **NOTE:** You must specify a file statement for the interface profile that has already been configured at the [edit accounting-options] hierarchy level. For more information, see the Configuring Accounting-Data Log Files.

3. Each interface with an accounting profile enabled has statistics collected once per interval time specified for the accounting profile. Statistics collection time is scheduled evenly over the configured interval. To configure the interval, include the interval statement at the [edit accounting-options interface-profile profile-name] hierarchy level.

   [edit accounting-options interface-profile profile-name]
   user@host# set interval minutes

   **NOTE:** The minimum interval allowed is 1 minute. Configuring a low interval in an accounting profile for a large number of interfaces might cause serious performance degradation.
4. To configure the interfaces on which the accounting needs to be performed, apply 
the interface profile to a logical interface by including the `accounting-profile` statement 
at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

```
[edit interfaces]
user@host# set interface-name unit logical-unit-number accounting-profile profile-name
```

**See Also**
- Accounting Options Overview
- Configuring Accounting-Data Log Files

**Displaying Accounting Profile for the Logical Interface**

**Purpose**
To display the configured accounting profile a particular logical interface at the `[edit
accounting-options interface-profile profile-name]` hierarchy level:

- interface-name—ge-1/0/1
- Logical unit number—1
- Interface profile —if_profile
- File name—if_stats
- Interval—15 minutes

**Action**
- Run the `show` command at the `[edit interfaces ge-1/0/1 unit 1]` hierarchy level.

```
[edit interfaces ge-1/0/1 unit 1]
accounting-profile if_profile;
```

- Run the `show` command at the `[edit accounting-options]` hierarchy level.

```
interface-profile if_profile {
  interval 15;
  file if_stats {
    fields {
      input-bytes;
      output-bytes;
      input-packets;
      output-packets;
      input-errors;
      output-errors;
    }
  }
}
```

**Meaning**
The configured accounting and its associated set options are displayed as expected.
Enabling or Disabling SNMP Notifications on Logical Interfaces

By default, Simple Network Management Protocol (SNMP) notifications are sent when the state of an interface or a connection changes. To explicitly enable these notifications on the logical interface, include the `traps` statement; to disable these notifications on the logical interface, include the `no-traps` statement:

```
(traps | no-traps);
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

Disabling a Logical Interface

You can unconfigure a logical interface, effectively disabling that interface, without removing the logical interface configuration statements from the configuration. To do this, include the `disable` statement:

```
disable;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

When an interface is disabled, a route (pointing to the reserved target “REJECT”) with the IP address of the interface and a 32–bit subnet mask is installed in the routing table. See Routing Protocols.

Example: Disabling a Logical Interface

Sample interface configuration:

```
[edit interfaces]
user@host# show
et-2/1/1 { 
  vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 0 { 
    vlan-id 1000;
    family inet { 
      address 11.0.0.20/24; 
      }
  }
}
```
Disabling the interface:

[edit interfaces et-2/1/1 unit 0]
user@host# set disable

Verifying the interface configuration:

[edit interfaces et-2/1/1]
user@host# show disable
disable; # Interface is marked as disabled.
unit 0 {
  vlan-id 1000;
  family inet {
    address 11.0.0.20/24;
  }
}

Configuring Logical System Interface Properties

With Junos OS, you can partition a single physical router into multiple logical devices that perform independent routing tasks. Because logical systems perform a subset of the tasks once handled by the physical router, logical systems offer an effective way to maximize the use of a single router.

1. Configure the physical interface that needs to be partitioned into multiple logical systems.

   [edit]
   user@host# set interfaces interface-name description description

2. Create the logical system interface on the logical unit.

   [edit]
   user@host# set logical-systems name interfaces interface-name unit logical-unit-number description description

3. Configure the required properties for the logical system.

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

Related Documentation
  • Setting Up Logical Systems
CHAPTER 4

Configuring Protocol Family and Interface Address Properties

- Protocol Family Configuration and Interface Address Statements on page 187
- Configuring the Protocol Family on page 190
- Configuring the Interface Address on page 191
- Configuring Default, Primary, and Preferred Addresses and Interfaces on page 193
- Operational Behavior of Interfaces When the Same IPv4 Address Is Assigned to Them on page 195
- Configuring ICCP for MC-LAG on page 198
- Configuring IPCP Options for Interfaces with PPP Encapsulation on page 200
- Configuring an Unnumbered Interface on page 202
- Setting the Protocol MTU on page 209
- Disabling the Removal of Address and Control Bytes on page 210
- Disabling the Transmission of Redirect Messages on an Interface on page 210
- Applying Policers on page 210
- Applying a Filter to an Interface on page 220
- Guidelines for Configuring Unicast RPF on ACX Series Routers on page 225
- Understanding Unicast RPF (Routers) on page 226
- Understanding and Preventing Unknown Unicast Forwarding on page 236
- Enabling Source Class and Destination Class Usage on page 241
- Understanding Targeted Broadcast on page 250
- Configuring Targeted Broadcast on page 251

Protocol Family Configuration and Interface Address Statements

For each logical interface, you must configure one or more protocol families. You can also configure interface address properties. To do this, include the following statements:

```plaintext
family family {
  accounting {
    destination-class-usage;
  }
}
```
source-class-usage {
    direction;
}
}

address address {
    destination address;
}

bundle interface-name;

filter {
    dialer filter-name;
    input filter-name;
    output filter-name;
    group filter-group-number;
}

interface-mode (access | trunk);

ipsec-sa sa-name;

keep-address-and-control;

mtu bytes;

multicast-only;

negociate-address;

no-redirects:

policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}

primary;

protocols [inet isompls];

proxy inet-address address;

receive-options-packets;

receive-ttl-exceeded;

remote (inet-address address | mac-address address);

rpf-check <fail-filter filter-name>;

sampling {
    direction;
}

service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
}

output {
    service-set service-set-name <service-filter filter-name>;
}

}

targeted-broadcast {
    forward-and-send-to-re;
    forward-only;
}

(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;

vlan-id number;

vlan-id-list [number number-number];
unnumbered-address interface-name destination address destination-profile profile-name;
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
broadcast address;
destination address;
destination-profile name;
eui-64;
multipoint-destination address dlci dlci-identifier;
multipoint-destination address {
    epd-threshold cells;
    inverse-arp;
oam-liveness {
        up-count cells;
        down-count cells;
    }
oam-period (disable | seconds);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
        queue-length number;
    }
    vci vpi-identifier.vci-identifier;
}
primary;
preferred;
(vrrp-group | vrrp-inet6-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    fast-interval milliseconds;
    (preempt | no-preempt) {
        hold-time seconds;
    }
    priority-number number;
    track {
        priority-cost seconds;
        priority-hold-time interface-name {
            interface priority;
            bandwidth-threshold bits-per-second {
                priority;
            }
        }
        route ip-address/mask routing-instance instance-name priority-cost cost;
    }
    virtual-address [ addresses ];
}
}

You can include these statements at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number]
• `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

For information about interface-specific protocol and address properties, see *Configuring T1 and NxDS0 Interfaces*.

**Related Documentation**

- *Configuring T1 and NxDS0 Interfaces*

## Configuring the Protocol Family

A protocol family is a group of logical properties within an interface configuration. Protocol families include all the protocols that make up a protocol suite. To use a protocol within a particular suite, you must configure the entire protocol family as a logical property for an interface.

Junos OS protocol families include the following common protocol suites:

- Inet—Supports IP protocol traffic, including OSPF, BGP, and Internet Control Message Protocol (ICMP).
- Inet6—Supports IPv6 protocol traffic, including RIP for IPv6 (RIPng), IS-IS, and BGP.
- ISO—Supports IS-IS traffic.
- MPLS—Supports MPLS.

In addition to the common protocol suites, JUNOS protocol families sometimes use the following protocol suites. For more information see, `family`.

To configure the logical interface’s protocol family, include the `family` statement, specifying the selected family. To configure the protocol family, following are the minimum configuration tasks under the `[edit interfaces interface-name unit logical-unit-number family family]` hierarchy.

### Table 23: Protocol Family Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Find Details Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MTU</td>
<td>“Configuring the Media MTU” on page 99</td>
</tr>
<tr>
<td>Configure the unit and family so that the interface can transmit and receive multicast traffic only</td>
<td><em>Restricting Tunnels to Multicast Traffic</em></td>
</tr>
<tr>
<td>Disable the sending of redirect messages by the router</td>
<td><em>Configuring Junos OS to Disable Protocol Redirect Messages on the Router or Switch</em></td>
</tr>
<tr>
<td>Assign an address to an interface</td>
<td>“Configuring the Interface Address” on page 191</td>
</tr>
</tbody>
</table>

**Related Documentation**

- `family` on page 603
Configuring the Interface Address

You assign an address to an interface by specifying the address when configuring the protocol family. For the **inet** or **inet6** family, configure the interface IP address. For the **iso** family, configure one or more addresses for the loopback interface. For the **ccc**, **ethernet-switching**, **tcc**, **mpls**, **tnp**, and **vpls** families, you never configure an address.

**NOTE:** The point-to-point (PPP) address is taken from the loopback interface address that has the primary attribute. When the loopback interface is configured as an unnumbered interface, it takes the primary address from the donor interface.

To assign an address to an interface, perform the following steps:
1. Configure the interface address at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level.
   - To configure an IPv4 address on routers and switches running Junos OS, use the interface interface-name unit number family inet address a.b.c.d/nn statement at the [edit interfaces] hierarchy level.

   You can also assign multiple IPv4 addresses on the same interface.

   [edit interfaces ]
   user@host# set interface-name unit logical-unit-number family inet address a.b.c.d/nn

   NOTE:
   - Juniper Networks routers and switches support /31 destination prefixes when used in point-to-point Ethernet configurations; however, they are not supported by many other devices, such as hosts, hubs, routers, or switches. You must determine if the peer system also supports /31 destination prefixes before configuration.
   - You can configure the same IPv4 address on multiple physical interfaces. When you assign the same IPv4 address to multiple physical interfaces, the operational behavior of those interfaces differs, depending on whether they are implicitly or explicitly point-to-point.
   - By default, all interfaces are assumed to be point-to-point (PPP) interfaces. For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, you can explicitly configure an interface to be a point-to-point connection.
   - If you configure the same IP address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration. The remaining IP address configurations are ignored, leaving some interfaces without an assigned address. Interfaces without an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

   [edit interfaces ]
   user@host# set interface-name unit logical-unit-number family inet6 address aaaa:bbbb:...:zzzz/nn

   NOTE:
   - To configure an IPv6 address on routers and switches running Junos OS, use the interface interface-name unit number family inet6 address aaaa:bbbb:...:zzzz/nn statement at the [edit interfaces] hierarchy level.

   [edit interfaces ]
   user@host# set interface-name unit logical-unit-number family inet6 address aaaa:bbbb:...:zzzz/nn

   NOTE:
   - You represent IP version 6 (IPv6) addresses in hexadecimal notation using a colon-separated list of 16-bit values. The double colon (::) represents all bits set to 0.
• You must manually configure the router or switch advertisement and advertise the default prefix for autoconfiguration to work on a specific interface.

2. [Optional] Set the broadcast address on the network or subnet.

   [edit interfaces interface-name unit logical-unit-number family family address address],
   user@host# set broadcast address

   NOTE: The broadcast address must have a host portion of either all ones or all zeros. You cannot specify the addresses 0.0.0.0 or 255.255.255.255

3. [Optional] specify the remote address of the connection for the encrypted, PPP-encapsulated, and tunnel interfaces.

   [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]
   user@host# set destination address

4. [Optional] For interfaces that carry IP version 6 (IPv6) traffic, configure the host to assign itself a unique 64-Bit IP Version 6 interface identifier (EUI-64).

   [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]
   user@host# set eui-64

Related Documentation
• Configuring Default, Primary, and Preferred Addresses and Interfaces on page 193

Configuring Default, Primary, and Preferred Addresses and Interfaces

• Default, Primary, and Preferred Addresses and Interfaces on page 193
• Configuring the Primary Interface for the Router on page 194
• Configuring the Primary Address for an Interface on page 194
• Configuring the Preferred Address for an Interface on page 195

Default, Primary, and Preferred Addresses and Interfaces

The router has a default address and a primary interface, and interfaces have primary and preferred addresses.

The default address of the router is used as the source address on unnumbered interfaces. The routing protocol process tries to pick the default address as the router ID, which is used by protocols, including OSPF and internal BGP (IBGP).
The primary interface for the router is the interface that packets go out when no interface name is specified and when the destination address does not imply a particular outgoing interface.

An interface’s primary address is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface. An interface’s preferred address is the default local address used for packets sourced by the local router to destinations on the subnet.

The default address of the router is chosen using the following sequence:

1. The primary address on the loopback interface lo0 that is not 127.0.0.1 is used.
2. The primary address on the primary interface is used.

Configuring the Primary Interface for the Router

The primary interface for the router has the following characteristics:

- It is the interface that packets go out when you type a command such as ping 255.255.255.255—that is, a command that does not include an interface name (there is no interface type-0/0/0.0 qualifier) and where the destination address does not imply any particular outgoing interface.
- It is the interface on which multicast applications running locally on the router, such as Session Announcement Protocol (SAP), do group joins by default.
- It is the interface from which the default local address is derived for packets sourced out an unnumbered interface if there are no non-127 addresses configured on the loopback interface, lo0.

By default, the multicast-capable interface with the lowest-index address is chosen as the primary interface. If there is no such interface, the point-to-point interface with the lowest index address is chosen. Otherwise, any interface with an address could be picked. In practice, this means that, on the router, the fxp0 or em0 interface is picked by default.

To configure a different interface to be the primary interface, include the primary statement:

```
primary;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family family]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]

Configuring the Primary Address for an Interface

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. For example, the local address in the packets sent by a ping interface so-0/0/0.0
255.255.255.255 command is the primary address on interface so-0/0/0. The primary address flag also can be useful for selecting the local address used for packets sent out unnumbered interfaces when multiple non-127 addresses are configured on the loopback interface, lo0. By default, the primary address on an interface is selected as the numerically lowest local address configured on the interface.

To set a different primary address, include the primary statement:

```
primary;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family family address address]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]

### Configuring the Preferred Address for an Interface

The preferred address on an interface is the default local address used for packets sourced by the local router to destinations on the subnet. By default, the numerically lowest local address is chosen. For example, if the addresses 172.16.1.1/12, 172.16.1.2/12, and 172.16.1.3/12 are configured on the same interface, the preferred address on the subnet (by default, 172.16.1.1) would be used as a local address when you issue a ping 172.16.1.5 command.

To set a different preferred address for the subnet, include the preferred statement:

```
preferred;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family family address address]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]

### Operational Behavior of Interfaces When the Same IPv4 Address Is Assigned to Them

You can configure the same IPv4 address on multiple physical interfaces. When you assign the same IPv4 address to multiple physical interfaces, the operational behavior of those interfaces differs, depending on whether they are implicitly or explicitly point-to-point.
NOTE: By default, all interfaces are assumed to be point-to-point (PPP) interfaces. For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, you can explicitly configure an interface to be a point-to-point connection.

NOTE: If you configure the same IP address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration. The remaining IP address configurations are ignored, leaving some interfaces without an assigned address. Interfaces without an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

In the following example, the IP address configuration for interface xe-0/0/1.0 is ignored:

```
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
}
```

The following examples show the sample configuration of assigning the same IPv4 address to implicitly and explicitly point-to-point interfaces, and their corresponding `show interfaces terse` command outputs to see their operational status.

```
[edit]
user@host# show
ge-0/1/0 {
  unit 0 {
    family inet {
      address 200.1.1.1/24;
    }
  }
}
ge-3/0/1 {
  unit 0 {
    family inet {
```
address 200.1.1.1/24;
}
}
}

The sample output shown below for the above configuration reveals that only ge-0/1/0.0 was assigned the same IPv4 address 200.1.1.1/24 and its link state was **up**, while ge-3/0/1.0 was not assigned the IPv4 address, though its link state was **up**, which means that it will be operational only when it gets a unique IPv4 address other than 200.1.1.1/24.

```bash
user@host> show interfaces terse ge*
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/1/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>200.1.1.1/24</td>
</tr>
<tr>
<td>ge-0/1/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/1</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-3/0/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-3/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-3/0/1.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[edit]
user@host# show
so-0/0/0 { 
    unit 0 { 
        family inet { 
            address 200.1.1.1/24; 
        } 
    } 
}

The sample output shown below for the above configuration reveals that both so-0/0/0.0 and so-0/0/3.0 were assigned the same IPv4 address 200.1.1.1/24 and that their link states were down, which means that to make them operational at least one of them will have to be configured with a unique IPv4 address other than 200.1.1.1/24.

```bash
user@host> show interfaces terse so*
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>so-0/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/2</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/3.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>so-1/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring ICCP for MC-LAG

For multichassis link aggregation (MC-LAG), you must configure Inter-Control Center Communications Protocol (ICCP) to exchange information between two MC-LAG peers.

To enable ICCP, include the `iccp` statement at the `[edit protocols]` hierarchy level:

```
[edit protocols]
iccp {
    authentication-key string;
    local-ip-addr ipv4-address;
    peer ip-address {
        authentication-key string;
        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 (1 | automatic);
        }
        local-ip-addr ipv4-address;
        redundancy-group-id-list [ redundancy-groups ];
        session-establishment-hold-time value;
    }
    session-establishment-hold-time value;
    traceoptions;
}
```

The `local-ip-address` statement sets the source address. This could be a specified address or interface address. The `session-establishment-hold-time` statement determines whether a chassis takes over as the master at the ICCP session.
The **authentication-key** statement is provided by TCP Message Digest 5 (md5) option for an ICCP TCP session. The **redundancy-group-id-list** statement specifies the redundancy groups between ICCP peers and the **liveness-detection** hierarchy configures Bidirectional Forwarding Detection (BFD) protocol options.

**NOTE:** ICCP is based on TCP and it uses IP routes to reach the MC-LAG peer. To ensure that the ICCP session is as resilient as possible, we recommend that you configure alternative routes between the ICCP end-point IP addresses. Alternatively, configure a LAG interface that has two or more interfaces between the MC-LAG pairs to prevent session failure when there are no alternative routes.

For Inter-Control Center Communications Protocol (ICCP) in a multichassis link aggregation group (MC-LAG) configured in an active-active bridge domain, you must ensure that you configure the same peer IP address hosting the MC-LAG by including the **peer ip-address** statement at the [edit protocols iccp] hierarchy level and the **multi-chassis-protection peer ip-address** statement at the [edit interfaces interface-name] hierarchy level. Multichassis protection reduces the configuration at the logical interface level for MX Series routers with multichassis aggregated Ethernet (MC-AE) interfaces. If the ICCP is UP and the interchassis data link (ICL) comes UP, the router configured as standby will bring up the MC-AE interfaces shared with the peer active-active node specified by the **peer** statement.

For example, the following statements illustrate how the same peer IP address can be configured for both the ICCP peer and multichassis protection link:

```
set interfaces ae1 unit 0 multi-chassis-protection 10.255.34.112 interface ae0
set protocols iccp peer 10.255.34.112 redundancy-group-id-list 1
```

Although you can commit an MC-LAG configuration with various parameters defined for it, you can configure multichassis protection between two peers without configuring the ICCP peer address. You can also configure multiple ICCP peers and commit such a configuration.

**Related Documentation**
Configuring IPCP Options for Interfaces with PPP Encapsulation

For interfaces with PPP encapsulation, you can configure IPCP to negotiate IP address assignments and to pass network-related information such as Windows Name Service (WINS) and Domain Name System (DNS) servers, as defined in RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*.

When you enable a PPP interface, you can configure an IP address, enable the interface to negotiate an IP address assignment from the remote end, or allow the interface to be unnumbered. You can also assign a destination profile to the remote end. The destination profile includes PPP properties, such as primary and secondary DNS and NetBIOS Name Servers (NBNSs). These options are described in the following sections:

**NOTE:** The Junos OS does not request name servers from the remote end; the software does, however, send name servers to the remote end if requested.

Before you begin

You must configure the PPP encapsulation on the interface before configuring the IPCP option. On the logical interface, the following PPP encapsulation types are supported:

- atm-mippp-llc
- atm-ppp-llc
- atm-ppp-vc-mux
- multilink-ppp

For more information about PPP encapsulation, see “Configuring Interface Encapsulation on Logical Interfaces” on page 173 and *Configuring ATM Interface Encapsulation*.

- To configure an IP address for the interface, include the `address` statement in the configuration. For more information, see “Configuring the Interface Address” on page 191.

If you include the `address` statement in the configuration, you cannot include the `negotiate-address` or `unnumbered-address` statement in the configuration.

When you include the `address` statement in the interface configuration, you can assign PPP properties to the remote end.

**NOTE:** The option to negotiate an IP address is not allowed in MLFR and MFR encapsulations.

- To enable the interface to obtain an IP address from the remote end, include the `negotiate-address` statement at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level.
NOTE: If you include the `negotiate-address` statement in the configuration, you cannot include the `address` or `unnumbered-address` statement in the configuration.

- To configure an interface to be unnumbered, include the `unnumbered-address` and `destination` statements in the configuration.

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

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

NOTE:
- The `unnumbered-address` statement enables the local address to be derived from the specified interface. The interface name must include a logical unit number and must have a configured address (see “Configuring the Interface Address” on page 191). Specify the IP address of the remote interface with the `destination` statement.
- If you include the `unnumbered-address` statement in the configuration, you cannot include the `address` or `negotiate-address` statement in the interface configuration.

- To assign PPP properties to the remote end include the `destination-profile` statement:

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

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name]
user@host# set destination-profile name
```

NOTE:
- You can assign PPP properties to the remote end, after you include the `address` or `unnumbered-address` statement in the interface configuration.
- You define the profile at the [edit access group-profile name ppp] hierarchy level. For more information, see Example: PPP MP for L2TP

Related Documentation
- Example: PPP MP for L2TP
- Configuring Interface Encapsulation on Logical Interfaces on page 173
Configuring an Unnumbered Interface

This topic includes the following information:

- Overview of Unnumbered Interfaces on page 202
- Configuring an Unnumbered Point-to-Point Interface on page 202
- Configuring an Unnumbered Ethernet or Demux Interface on page 203
- Configuring a Preferred Source Address for Unnumbered Ethernet or Demux Interfaces on page 204
- Restrictions for Configuring Unnumbered Ethernet Interfaces on page 205
- Displaying the Unnumbered Ethernet Interface Configuration on page 206
- Displaying the Configured Preferred Source Address for an Unnumbered Ethernet Interface on page 207
- Displaying the Configuration for Unnumbered Ethernet Interface as the Next Hop for a Static Route on page 208

Overview of Unnumbered Interfaces

When you need to conserve IP addresses, you can configure unnumbered interfaces. Setting up an unnumbered interface enables IP processing on the interface without assigning an explicit IP address to the interface. For IPv6, in which conserving addresses is not a major concern, you can configure unnumbered interfaces to share the same subnet across multiple interfaces. IPv6 unnumbered interfaces are only supported on Ethernet interfaces. The statements you use to configure an unnumbered interface depend on the type of interface you are configuring: a point-to-point interface or an Ethernet interface:

Configuring an Unnumbered Point-to-Point Interface

1. In configuration mode, go to the `edit interfaces interface-name unit logical-unit-number` hierarchy level.
   
   ```
   [edit ]
   user@host# edit interfaces interface-name unit logical-unit-number
   ```

2. To configure an unnumbered point-to-point interface, configure the protocol family, but do not include the `address` statement.
   
   ```
   [edit interfaces interface-name unit logical-unit-number]
   user@host# set family
   ```
NOTE:

- For interfaces with PPP encapsulation, you can configure an unnumbered interface by including the `unnumbered-interface` statement in the configuration. For more information, see “Configuring IPCP Options for Interfaces with PPP Encapsulation” on page 200.

- When configuring unnumbered interfaces, you must ensure that a source address is configured on some interface in the router. This address is the default address. We recommend that you do this by assigning an address to the loopback interface (lo0), as described in “Loopback Interface Configuration” on page 310. If you configure an address (other than a martian) on the lo0 interface, that address is always the default address, which is preferable because the loopback interface is independent of any physical interfaces and therefore is always accessible.

Configuring an Unnumbered Ethernet or Demux Interface

1. In configuration mode, go to the `[edit interfaces interface-name unit logical-unit-number family family-name]` hierarchy level.
   
   [edit ]
   user@host# edit interfaces interface-name unit logical-unit-number family family-name

2. To configure an unnumbered Ethernet or demultiplexing interface, include the `unnumbered-address` statement in the configuration.
   
   [edit interfaces interface-name unit logical-unit-number family family-name]
   user@host# set unnumbered-address interface-name

3. (Optional) To specify the unnumbered Ethernet interface as the next-hop interface for a configured static route, include the `qualified-next-hop` statement at the `[edit routing-options static route destination-prefix]` hierarchy level. This feature enables you to specify independent preferences and metrics for static routes on a next-hop basis.
   
   [edit routing-options static route destination-prefix]
   user@host# set qualified-next-hop (address | interface-name)
**NOTE:**

- The **unnumbered-address** statement currently supports configuration of unnumbered demux interfaces only for the IPv4 address family. You can configure unnumbered Ethernet interfaces for both IPv4 and IPv6 address families.

- The interface that you configure to be unnumbered **borrows** an assigned IP address from another interface, and is referred to as the **borrower interface**. The interface from which the IP address is borrowed is referred to as the **donor interface**. In the **unnumbered-address** statement, `interface-name` specifies the donor interface. For an unnumbered Ethernet interface, the donor interface can be an Ethernet, ATM, SONET, or loopback interface that has a logical unit number and configured IP address and is not itself an unnumbered interface. For an unnumbered IP demultiplexing interface, the donor interface can be an Ethernet or loopback interface that has a logical unit number and configured IP address and is not itself an unnumbered interface. In addition, for either Ethernet or demux, the donor interface and the borrower interface must be members of the same routing instance and the same logical system.

- When you configure an unnumbered Ethernet or demux interface, the IP address of the donor interface becomes the source address in packets generated by the unnumbered interface.

- You can configure a host route that points to an unnumbered Ethernet or demux interface. For information about host routes, see the *MPLS Applications Feature Guide*.

---

**Configuring a Preferred Source Address for Unnumbered Ethernet or Demux Interfaces**

When a loopback interface with multiple secondary IP addresses is configured as the donor interface for an unnumbered Ethernet or demux interface, you can optionally specify any one of the loopback interface's secondary addresses as the preferred source address for the unnumbered Ethernet or demux interface. This feature enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet or demux interfaces in your network.

1. In configuration mode, go to the `edit interfaces interface-name unit logical-unit-number family family-name` hierarchy level.

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

2. To configure a secondary address on a loopback donor interface as the preferred source address for an unnumbered Ethernet or demux interface, include the `preferred-source-address` option in the `unnumbered-address` statement:

   ```
   [edit interfaces interface-name unit logical-unit-number family family-name]
   ```
user@host# set unnumbered-address interface-name <preferred-source-address>

NOTE:
The following considerations apply when you configure a preferred source address on an unnumbered Ethernet or demux interface:

- The unnumbered-address statement currently supports the configuration of a preferred source address only for the IPv4 address family for demux interfaces, and for IPv4 and IPv6 address families for Ethernet interfaces.
- If you do not specify the preferred source address, the router uses the default primary IP address of the donor interface.
- You cannot delete an address on a donor loopback interface while it is being used as the preferred source address for an unnumbered Ethernet or demux interface.

Restrictions for Configuring Unnumbered Ethernet Interfaces

The following restrictions apply when you configure unnumbered Ethernet interfaces:

- The unnumbered-address statement currently supports the configuration of unnumbered Ethernet interfaces for IPv4 and IPv6 address families.
- You cannot assign an IP address to an Ethernet interface that is already configured as an unnumbered interface.
- The donor interface for an unnumbered Ethernet interface must have one or more configured IP addresses.
- The donor interface for an unnumbered Ethernet interface cannot be configured as unnumbered.
- An unnumbered Ethernet interface does not support configuration of the following address statement options: arp, broadcast, primary, preferred, and vrrp-group. For information about these options, see “Configuring the Interface Address” on page 191.
- Running IGMP and PIM are supported only on unnumbered Ethernet interfaces that directly face the host and have no downstream PIM neighbors. IGMP and PIM are not supported on unnumbered Ethernet interfaces that act as upstream interfaces in a PIM topology.
- Running OSPF and IS-IS on unnumbered Ethernet interfaces is not supported. However, you can run OSPF over unnumbered Ethernet interfaces configured as a Point-to-Point connection.

For link-state distribution using an interior gateway protocol (IGP), ensure that OSPF is enabled on the donor interface for an unnumbered interface configuration, so the donor IP address is reachable to establish OSPF sessions.
NOTE: If you configure the same address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration, the remaining address configurations are ignored and can leave interfaces without an address. Interfaces that do not have an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

For example, in the following configuration the address configuration of interface xe-0/0/1.0 is ignored:

```conf
textcolor:gray
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
}
```

For more information on configuring the same address on multiple interfaces, see "Configuring the Interface Address" on page 191.

Displaying the Unnumbered Ethernet Interface Configuration

**Purpose** To display the configured unnumbered interface at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

- Unnumbered interface —ge-1/0/0
- Donor interface —ge-0/0/0
- Donor interface address —4.4.4.1/24

The unnumbered interface "borrows" an IP address from the donor interface.

**Action** Run the show command at the [edit] hierarchy level.

```conf
textcolor:gray
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 4.4.4.1/24;
      }
    }
  }
  ge-1/0/0 {
```
Meaning

The sample configuration that is described works correctly on M and T Series routers. For unnumbered interfaces on MX Series routers, you must additionally configure static routes on an unnumbered Ethernet interface by including the `qualified-next-hop` statement at the `[edit routing-options static route destination-prefix]` hierarchy level to specify the unnumbered Ethernet interface as the next-hop interface for a configured static route.

Displaying the Configured Preferred Source Address for an Unnumbered Ethernet Interface

**Purpose**

To display the configuration of preferred source address for an unnumbered interface at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level:

- Unnumbered interface — `ge-4/0/0`
- Donor interface — `lo0`
- Donor interface primary address — `2.2.2.1/32`
- Donor interface secondary address — `3.3.3.1/32`

**Action**

Run the `show` command at the `[edit]` hierarchy level.

```plaintext
interfaces {
    lo0 {
        unit 0 {
            family inet {
                address 2.2.2.1/32;
                address 3.3.3.1/32;
            }
        }
    }
    interfaces {
        ge-4/0/0 {
            unit 0 {
                family inet {
                    unnumbered-address lo0.0 preferred-source-address 3.3.3.1;
                }
            }
        }
    }
}
```
Meaning  The loopback interface lo0 is the donor interface from which unnumbered Ethernet interface ge-4/0/0 “borrows” an IP address.

The example shows one of the loopback interface’s secondary addresses, 3.3.3.1, as the preferred source address for the unnumbered Ethernet interface.

Displaying the Configuration for Unnumbered Ethernet Interface as the Next Hop for a Static Route

Purpose  To display the unnumbered interface configured as the next hop for the static route at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level:

- Unnumbered interface —ge-0/0/0
- Donor interface —lo0
- Donor interface primary address—5.5.5.1/32
- Donor interface secondary address—6.6.6.1/32
- Static route—7.7.7.1/32

Action  • Run the show command at the [edit] hierarchy level.

```bash
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 5.5.5.1/32;
        address 6.6.6.1/32;
      }
    }
  }
}

static {
  route 7.7.7.1/32 {
    qualified-next-hop ge-0/0/0.0;
  }
}
```

• The following configuration enables the kernel to install a static route to address 7.7.7.1/32 with a next hop through unnumbered interface ge-0/0/0.0.
Meaning

In this example, `ge-0/0/0` is the unnumbered interface and a loopback interface, `lo0`, is the donor interface from which `ge-0/0/0` “borrows” an IP address. The example also configures a static route to `7.7.7.1/32` with a next hop through unnumbered interface `ge-0/0/0.0`.

Setting the Protocol MTU

When you initially configure an interface, the protocol maximum transmission unit (MTU) is calculated automatically. If you subsequently change the media MTU, the protocol MTU on existing address families automatically changes.

For a list of default protocol MTU values, see “Media MTU Sizes by Interface Type” on page 85.

To modify the MTU for a particular protocol family, include the `mtu` statement:

```
mtu bytes;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

If you increase the size of the protocol MTU, you must ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. For a list of encapsulation overhead values, see “Encapsulation Overhead by Interface Encapsulation Type” on page 97. If you reduce the media MTU size, but there are already one or more address families configured and active on the interface, you must also reduce the protocol MTU size. (You configure the media MTU by including the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level.)

NOTE: Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

The maximum number of data-link connection identifiers (DLCIs) is determined by the MTU on the interface. If you have keepalives enabled, the maximum number of DLCIs is 1000, with the MTU set to 5012.

The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the MTU. For example, the default protocol MTU for a Gigabit Ethernet interface is 1500 bytes, but the largest possible frame size is actually 1504 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.

Related Documentation

- Media MTU Overview on page 84
**Disabling the Removal of Address and Control Bytes**

For Point-to-Point Protocol (PPP) CCC-encapsulated interfaces, the address and control bytes are removed by default before the packet is encapsulated into a tunnel.

You can disable the removal of address and control bytes. To do this, include the `keep-address-and-control` statement:

```
keep-address-and-control;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family ccc]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family ccc]`

**Related Documentation**
- `keep-address-and-control` on page 717

**Disabling the Transmission of Redirect Messages on an Interface**

By default, the interface sends protocol redirect messages. To disable the sending of these messages on an interface, include the `no-redirects` statement:

```
no-redirects;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

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

**Related Documentation**
- `no-redirects` on page 840

**Applying Policers**

- Overview of Applying Policers on page 211
- Applying Aggregate Policers on page 212
- Applying Hierarchical Policers on Enhanced Intelligent Queuing PICs on page 214
- Configuring Hierarchical Policers on page 216
- Configuring a Single-Rate Two-Color Policer on page 217
Overview of Applying Policers

Policers allow you to perform simple traffic policing on specific interfaces or Layer 2 virtual private networks (VPNs) without configuring a firewall filter. To apply policers, include the `policer` statement:

```plaintext
policer {
  arp policer-template-name;
  input policer-template-name;
  output policer-template-name;
}
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

In the `family` statement, the protocol family can be `ccc`, `inet`, `inet6`, `mpls`, `tcc`, or `vpls`.

In the `arp` statement, list the name of one policer template to be evaluated when Address Resolution Protocol (ARP) packets are received on the interface. By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the `family inet` statement. If you want more stringent or lenient policing of ARP packets, you can configure an interface-specific policer and apply it to the interface. You configure an ARP policer just as you would configure any other policer, at the `[edit firewall policer]` hierarchy level. If you apply this policer to an interface, the default ARP packet policer is overridden. If you delete this policer, the default policer takes effect again.

In the `input` statement, list the name of one policer template to be evaluated when packets are received on the interface.

In the `output` statement, list the name of one policer template to be evaluated when packets are transmitted on the interface.

**NOTE:** To use policing on a CCC or TCC interface, you must configure the CCC or TCC protocol family.

You can configure a different policer on each protocol family on an interface, with one input policer and one output policer for each family. When you apply policers, you can configure the family `ccc`, `inet`, `inet6`, `mpls`, `tcc`, or `vpls` only, and one ARP policer for the family `inet` protocol only. Each time a policer is referenced, a separate copy of the policer is installed on the packet forwarding components for that interface.
If you apply both policers and firewall filters to an interface, input policers are evaluated before input firewall filters, and output policers are evaluated after output firewall filters.

If you apply the policer to the interface lo0, it is applied to packets received or transmitted by the Routing Engine.

On T Series, M120, and M320 platforms, if the interfaces are on the same FPC, the filters or policers do not act on the sum of traffic entering and exiting the interfaces.

For more information about policers, see the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide.

Applying Aggregate Policers

• Applying Aggregate Policers on page 212

Applying Aggregate Policers

By default, if you apply a policer to multiple protocol families on the same logical interface, the policer restricts traffic for each protocol family individually. For example, a policer with a 50 Mbps bandwidth limit applied to both IPv4 and IPv6 traffic would allow the interface to accept 50 Mbps of IPv4 traffic and 50 Mbps of IPv6 traffic. If you apply an aggregate policer, the policer would allow the interface to receive only 50 Mbps of IPv4 and IPv6 traffic combined.

To configure an aggregate policer, include the logical-interface-policer statement at the [edit firewall policer policer-template-name] hierarchy level:

[edit firewall policer policer-template-name]
logical-interface-policer;

For the policer to be treated as an aggregate, you must apply it to multiple protocol families on a single logical interface by including the policer statement:

policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}

You can include these statements at the following hierarchy levels:

• [edit interfaces interface-name unit logical-unit-number family family]
• [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]

In the family statement, the protocol family can be ccc, inet, inet6, mpls, tcc, or vpls.

The protocol families on which you do not apply the policer are not affected by the policer. For example, if you configure a single logical interface to accept MPLS, IPv4, and IPv6 traffic and you apply the logical interface policer policer1 to only the IPv4 and IPv6 protocol families, MPLS traffic is not subject to the constraints of policer1.
If you apply `policer1` to a different logical interface, there are two instances of the policer. This means the Junos OS polices traffic on separate logical interfaces separately, not as an aggregate, even if the same logical-interface policer is applied to multiple logical interfaces on the same physical interface port.

**Example: Applying Aggregate Policers**

Configure two logical interface policers: `aggregate_police1` and `aggregate_police2`. Apply `aggregate_police1` to IPv4 and IPv6 traffic received on logical interface `fe-0/0/0.0`. Apply `aggregate_police2` to CCC and MPLS traffic received on logical interface `fe-0/0/0.0`. This configuration causes the software to create only one instance of `aggregate_police1` and one instance of `aggregate_police2`.

Apply `aggregate_police1` to IPv4 and IPv6 traffic received on another logical interface `fe-0/0/0.1`. This configuration causes the software to create a new instance of `aggregate_police1`, one that applies to unit 0 and another that applies to unit 1.

```bash
[edit firewall]
policer aggregate_police1 {
    logical-interface-policer;
    if-exceeding {
        bandwidth-limit 100m;
        burst-size-limit 500k;
    }
    then {
        discard;
    }
}
policer aggregate_police2 {
    logical-interface-policer;
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 200k;
    }
    then {
        discard;
    }
}
[edit interfaces fe-0/0/0]
unit 0 {
    family inet {
        policer {
            input aggregate_police1;
        }
    }
    family inet6 {
        policer {
            input aggregate_police1;
        }
    }
    family ccc {
        policer {
            input aggregate_police2;
        }
    }
}`
Applying Hierarchical Policers on Enhanced Intelligent Queuing PICs

- Applying Hierarchical Policers on Enhanced Intelligent Queuing PICs on page 214

Applying Hierarchical Policers on Enhanced Intelligent Queuing PICs

M40e, M120, and M320 edge routers and T Series core routers with Enhanced Intelligent Queuing (IQE) PICs support hierarchical policers in the ingress direction and allow you to apply a hierarchical policer for the premium and aggregate (premium plus normal) traffic levels to an interface. Hierarchical policers provide cross-functionality between the configured physical interface and the Packet Forwarding Engine.

Before you begin, there are some general restrictions that apply to hierarchical policers:

- Only one type of policer can be configured for a logical or physical interface. For example, a hierarchical policer and a regular policer in the same direction for the same logical interface is not allowed.
- The chaining of the policers—that is, applying policers to both a port and the logical interfaces of that port—is not allowed.
- There is a limit of 64 policers per interface in case there is no BA classification, providing a single policer per DLCI.
- Only one kind of policer can be applied on a physical or logical interface.
- The policer should be independent of BA classification. Without BA classification, all traffic on an interface will be treated either as EF or non-EF, based on the configuration. With BA classification, an interface can support up to 64 policers. Again, the interface here may be a physical interface or logical interface (for example, DLCI).
- With BA classification, the miscellaneous traffic (the traffic not matching with any of the BA classification DSCP/EXP bits) will be policed as non-EF traffic. No separate policers will be installed for this traffic.
Hierarchical Policer Overview

Hierarchical policing uses two token buckets, one for aggregate (non-EF) traffic and one for premium (EF) traffic. Which traffic is EF and which is non-EF is determined by the class-of-service configuration. Logically, hierarchical policing is achieved by chaining two policers.

Figure 11: Hierarchical Policer

+ EF Traffic + Premium Policer

+ non-EF Traffic + Aggregate Policer

In the example in Figure 11 on page 215, EF traffic is policed by Premium Policer and non EF traffic is policed by Aggregate Policer. What that means is, for EF traffic the out-of-spec action will be the one that is configured for Premium Policer, but the in-spec EF traffic will still consume the tokens from the Aggregate Policer.

But EF traffic will never be submitted to the out-of-spec action of the Aggregate Policer. Also, if the out-of-spec action of the Premium Policer is not set to Discard, those out-of-spec packets will not consume the tokens from the Aggregate Policer. Aggregate Policer only polices the non-EF traffic. As you can see, the Aggregate Policer token bucket can go negative, if all the tokens are consumed by the non-EF traffic and then you get bursts of EF traffic. But that will be for a very short time, and over a period of time it will average out. For example:

- **Premium Policer**: Bandwidth 2 Mbps, OOS Action: Discard
- **Aggregate Policer**: Bandwidth 10 Mbps, OOS Action: Discard

In the above case, EF traffic is guaranteed 2 Mbps and the non-EF traffic will get from 8 Mbps to 10 Mbps, depending on the input rate of the EF traffic.

Hierarchical Policing Characteristics

Hierarchical token bucket features include:

- Ingress traffic is first classified into EF and non-EF traffic prior to applying a policer:
  - Classification is performed by Q-tree lookup
- Channel number selects a shared token bucket policer:
  - Dual token bucket policer is divided into two single bucket policers:
    - Policer1—EF traffic
    - Policer2—non-EF traffic
- Shared token bucket is used to police the traffic as follows:
  - Policer1 is set to EF rate (for example, 2 Mbps)
  - Policer2 is set to aggregate interface policed rate (for example, 10 Mbps).
• EF traffic gets applied to Policer1.
  • If traffic is in-spec it is allowed to pass and decrement from both Policer1 and Policer2.
  • If traffic is out-of-spec it can be discarded or marked with a new FC or loss priority. Policer2 will not do anything with out-of-spec EF traffic.

• Non-EF traffic gets applied only to Policer2.
  • If traffic is in-spec it is allowed to pass through and decremented Policer2.
  • If traffic is out-of-spec it is discarded or marked with a new FC or set with a new drop priority.

• Rate-limit the port speed to a desired rate at Layer 2
• Rate-limit the EF traffic
• Rate-limit the non-EF traffic
• Policing drops counted per color

See Also • Class of Service Feature Guide (Routers and EX9200 Switches)

Configuring Hierarchical Policers

To configure a hierarchical policer, apply the policing-priority statement to the proper forwarding class and configure a hierarchical policer for the aggregate and premium level. For more information about class of service, see the Class of Service Feature Guide (Routers and EX9200 Switches).

NOTE: Hierarchical policers can only be configured on SONET physical interfaces hosted on an IQE PIC. Only aggregate and premium levels are supported.

CoS Configuration of Forwarding Classes for Hierarchical Policers

[edit class-of-service forwarding-classes]
class fc1 queue-num 0 priority high policing-priority premium;
class fc2 queue-num 1 priority low policing-priority normal;
class fc3 queue-num 2 priority low policing-priority normal;
class fc4 queue-num 3 priority low policing-priority normal;

For detailed information on class-of-service configuration and statements, see the Class of Service Feature Guide (Routers and EX9200 Switches).

Firewall Configuration for Hierarchical Policers

[edit firewall hierarchical-policer foo]
aggregate {
  if-exceeding {
    bandwidth-limit 70m;
    burst-size-limit 1500;
  }
You can apply the hierarchical policer as follows:

```
[edit interfaces so-0/1/0 unit 0 layer2-policer]
input-hierarchical-policer foo;
```

You also have the option to apply the policer at the physical port level as follows:

```
[edit interfaces so-0/1/0 layer2-policer]
input-hierarchical-policer foo;
```

### Configuring a Single-Rate Two-Color Policer

You can configure a single-rate two-color policer as follows:

```
[edit firewall policer foo]
if-exceeding {
    bandwidth-limit 50m;
    burst-size-limit 1500;
}
then {
    discard;
}
```

You can apply the policer as follows:

```
[edit interfaces so-0/1/0 unit 0 layer2-policer]
input-policer foo;
```

You also have the option to apply the policer at the physical port level as follows:

```
[edit interfaces so-0/1/0 layer2-policer]
input-policer foo;
```

### Configuring a Single-Rate Color-Blind Policer

This section describes single-rate color blind and color aware policers.

You can configure a single-rate color blind policer as follows:
You can apply the single-rate color blind policer as follows:

[edit firewall three-color-policer foo]
  single-rate {
    color-blind;
    committed-information-rate 50m;
    committed-burst-size 1500;
    excess-burst-size 1500;
  }

You can apply the single-rate color-aware policer as follows:

[edit firewall three-color-policer bar]
  single-rate {
    color-aware;
    committed-information-rate 50m;
    committed-burst-size 1500;
    excess-burst-size 1500;
  }

You can configure a single-rate color-aware policer as follows:

[edit interfaces so-0/1/0 unit 0 layer2-policer]
  input-three-color foo;

You also have the option to apply the policer at the physical port level as follows:

[edit interfaces so-0/1/0 layer2-policer]
  input-three-color bar;

**Configuring a Two-Rate Tricolor Marker Policer**

Ingress policing is implemented using a two-rate tricolor marker (trTCM). This is done with a dual token bucket (DTB) that maintains two rates, committed, and a peak. Egress static policing also uses a token bucket.

The token buckets perform the following ingress policing functions:

- (1K) trTCM - Dual token bucket (red, yellow, and green marking)
- Policing is based on Layer 2 packet size:
  - After +/- byte adjust offset
- Marking is color aware and color blind:
  - Color aware needs to have the color set by q-tree lookup based on:
    - ToS
**EXP**

- Programmable marking actions:
  - **Color** (red, yellow, green)
  - Drop based on color and congestion profile

- Policer is selected based on the arriving channel number:
  - Channel number LUT produces policer index and queue index
  - Multiple channels can share the same policer (LUT produces same policer index)

- Support ingress policing and trTCM at the following levels:
  - Queue
  - Logical interface (ifl/DLCI)
  - Physical interface (ifd)
  - Physical port (controller ifd)
  - Any combinations of logical interface, physical interface, and port

- Support percentage of interface speed and bits per second

Rate limits may be applied to selected queues on ingress and on predefined queues at egress. The token bucket operates in color aware and color blind modes (specified by RFC 2698).

### Configuring a Color-Blind trTCM

```plaintext
[edit firewall three-color-policer foo]
two-rate {
  color-blind;
  committed-information-rate 50m;
  committed-burst-size 1500;
  peak-information-rate 100m;
  peak-burst-size 3k;
}
```

You can apply the three-color two-rate color-blind policer as follows:

```plaintext
[edit interfaces so-0/1/0 unit 0 layer2-policer]
input-three-color foo;
```

You also have the option to apply the policer at the physical port level as follows:

```plaintext
[edit interfaces so-0/1/0 layer2-policer]
input-three-color foo;
```

### Configuring a Color-Aware trTCM

```plaintext
[edit firewall three-color-policer bar]
two-rate {
  color-aware;
  committed-information-rate 50m;
}
```
committed-burst-size 1500;
peak-information-rate 100m;
peak-burst-size 3k;
}

You can apply the three-color two-rate color-aware policer as follows:

[edit interfaces so-0/1/0 unit 0 layer2-policer]
input-three-color bar;

You also have the option to apply the policer at the physical port level as follows:

[edit interfaces so-0/1/0 layer2-policer]
input-three-color bar;

See Also • Class of Service Feature Guide (Routers and EX9200 Switches)

Applying a Filter to an Interface

• Defining Interface Groups in Firewall Filters on page 220
• Applying a Filter to an Interface on page 221

Defining Interface Groups in Firewall Filters

When applying a firewall filter, you can define an interface to be part of an interface group. Packets received on that interface are tagged as being part of the group. You can then match these packets using the interface-group match statement, as described in the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide.

To define the interface to be part of an interface group, include the group statement:

    group filter-group-number;

You can include this statement at the following hierarchy levels:

• [edit interfaces interface-name unit logical-unit-number family family filter]
• [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family filter]

NOTE: The number 0 is not a valid interface group number.

Filter-Based Forwarding on the Output Interface

If port-mirrored packets are to be distributed to multiple monitoring or collection interfaces, based on patterns in packet headers, it is helpful to configure a filter-based forwarding (FBF) filter on the port-mirroring egress interface.
When an FBF filter is installed as an output filter, a packet that is forwarded to the filter has already undergone at least one route lookup. After the packet is classified at the egress interface by the FBF filter, it is redirected to another routing table for additional route lookup. To avoid packet looping inside the Packet Forwarding Engine, the route lookup in the latter routing table (designated by an FBF routing instance) must result in a different next hop from any next hop specified in a table that has already been applied to the packet.

If an input interface is configured for FBF, the source lookup is disabled for those packets headings to a different routing instance, since the routing table is not set up to handle the source lookup.

For more information about FBF configuration, see the Junos OS Routing Protocols Library. For more information about port mirroring, see the Junos OS Services Interfaces Library for Routing Devices.

Applying a Filter to an Interface

To apply firewall filters to an interface, include the `filter` statement:

```plaintext
filter {
  group filter-group-number;
  input filter-name;
  input-list [ filter-names ];
  output filter-name;
  output-list [ filter-names ];
}
```

To apply a single filter, include the `input` statement:

```plaintext
filter {
  input filter-name;
}
```

To apply a list of filters to evaluate packets received on an interface, include the `input-list` statement.

```plaintext
filter {
  input-list [ filter-names ];
}
```

Up to 16 filter names can be included in an input list.

To apply a list of filters to evaluate packets transmitted on an interface, include the `output-list` statement.

```plaintext
filter {
  output-list [ filter-names ];
}
```
When you apply filters using the `input-list` statement or the `output-list` statement, a new filter is created with the name `<interface-name>.<unit-direction>`. This filter is exclusively interface-specific.

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

In the `family` statement, the protocol family can be `ccc`, `inet`, `inet6`, `mpls`, or `vpls`.

In the `group` statement, specify the interface group number to associate with the filter.

In the `input` statement, list the name of one firewall filter to be evaluated when packets are received on the interface.

In the `input-list` statement, list the names of filters to evaluate when packets are received on the interface. You can include up to 16 filter names.

In the `output` statement, list the name of one firewall filter to be evaluated when packets are transmitted on the interface.

In the `output-list` statement, list the names of filters to evaluate when packets are transmitted on the interface. You can include up to 16 filter names.

You can use the same filter one or more times. On M Series routers (except the M320 and M120 routers), if you apply a firewall filter or policer to multiple interfaces, the filter or policer acts on the sum of traffic entering or exiting those interfaces.

On T Series, M120, and M320 routers, interfaces are distributed among multiple packet forwarding components. Therefore, on these routers, if you apply a firewall filter or policer to multiple interfaces, the filter or policer acts on the traffic stream entering or exiting each interface, regardless of the sum of traffic on the multiple interfaces.
For more information on Understanding Ethernet Frame Statistics, see the MX Series Layer 2 Configuration Guide.

If you apply the filter to the interface lo0, it is applied to packets received or transmitted by the Routing Engine. You cannot apply MPLS filters to the management interface (fxp0 or em0) or the loopback interface (lo0).

Filters applied at the [set interfaces lo0 unit 0 family any filter input] hierarchy level are not installed on T4000 Type 5 FPCs.

For more information about firewall filters, see the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide. For more information about MPLS filters, see the MPLS Applications Feature Guide.

Example: Input Filter for VPLS Traffic

For M Series and T Series routers only, apply an input filter to VPLS traffic. Output filters do not work for broadcast and multicast traffic, including VPLS traffic. Note that on MX Series routers with MPC/MIC interfaces, the VPLS filters on the egress is applicable to broadcast, multicast, and unknown unicast traffic.

```plaintext
[edit interfaces]
fe-2/2/3 {
    vlan-tagging;
    encapsulation vlan-vpls;
    unit 601 {
        encapsulation vlan-vpls;
        vlan-id 601;
        family vpls {
            filter {
                input filter1; # Works for multicast destination MAC address
                output filter1; # Does not work for multicast destination MAC address
            }
        }
    }
}
[edit firewall]
family vpls {
    filter filter1 {
        term 1 {
            from {
                destination-mac-address {
                    01:00:0c:cc:cc:cd/48;
                }
            }
            then {
                discard;
            }
        }
        term 2 {
            then {
                accept;
            }
        }
    }
}
```
Example: Filter-Based Forwarding at the Output Interface

The following example illustrates the configuration of filter-based forwarding at the output interface. In this example, the packet flow follows this path:

1. A packet arrives at interface \textit{fe-1/2/0.0} with source and destination addresses 10.50.200.1 and 10.50.100.1 respectively.
2. The route lookup in routing table \textit{inet.0} points to the egress interface \textit{so-0/0/3.0}.
3. The output filter installed at \textit{so-0/0/3.0} redirects the packet to routing table \textit{fbf.inet.0}.
4. The packet matches the entry 10.50.100.0/25 in the \textit{fbf.inet.0} table, and finally leaves the router from interface \textit{so-2/0/0.0}.

```plaintext
[edit interfaces]
so-0/0/3 {  
  unit 0 {  
    family inet {  
      filter {  
        output fbf;  
      }  
      address 10.50.10.2/25;  
    }  
  }  
}  
fe-1/2/0 {  
  unit 0 {  
    family inet {  
      address 10.50.50.2/25;  
    }  
  }  
}  
so-2/0/0 {  
  unit 0 {  
    family inet {  
      address 10.50.20.2/25;  
    }  
  }  
}  
[edit firewall]
filter fbf {  
  term 0 {  
    from {  
      source-address {  
        10.50.200.0/25;  
      }  
    }  
    then routing-instance fbf;  
  }  
  term d {  
    then count d;  
  }  
}  
[edit routing-instances]
fbf {
```
Guidelines for Configuring Unicast RPF on ACX Series Routers

Observe the following guidelines while configuring unicast RPF on ACX Series routers:

- Support for physical interfaces impacts inet families only.
- The RPF check to be used when routing is asymmetrical is not supported because the `unicast-reverse-path (active-paths | feasible-paths)` statement at the `[edit routing-instances routing-instance-name instance-type name routing-options forwarding-table]` hierarchy level is not supported.
- Even if uRPF checking is enabled, the reverse path checking is not performed if the following conditions apply:
  - The destination IP address is not a unicast address. This applies for both IPV4 and IPV6 packets.
  - The source IP address is IPV6 and the address is a link local address (FE80::/10)
  - The received packet is a BOOTP/DHCP packet (SIP=0.0.0.0 and DIP=255.255.255.255)
- If you enable/disable unicast RPF on live traffic, some packets are dropped while the packet forwarding components are updating. This behavior occurs because route reinstallation is initiated while you enable or disable uRPF.
- uRPF is supported at the logical interface level. Due to hardware limitations, support is available only at the logical interface level.
- Strict mode on ECMP routes is not supported in ACX. This condition occurs because the hardware treats ECMP routes as Loose Mode although the port is configured as Strict mode. Because ECMP uses multiple physical paths for the route the reverse path check results in utilizing many paths (routes) and the source port validation method.
is not used in case of Strict mode. As a result, such a network scenario operates in the same manner as loose mode.

- When the strict mode is enabled on the interface, if the packet is coming with an SIP address which ARP resolution is pending will be dropped as it points to RESOLVE_NH.
- uRPF fail filter can be configured for family `<inet | inet6>` in ACX.

NOTE: The uRPF fail filter cannot match packets failed at ingress port check (strict mode).

The uRPF fail filter can match packets failing source IP lookup but cannot match packets failing the input interface check (strict mode).

The uRPF fail filter applies only to interface-specific instances of the firewall filter.

The uRPF fail filters do not support reject and routing-instance actions.

- uRPF can be configured for family `<inet | inet6>` on IRB interfaces in ACX.
- uRPF implementation in ACX does not consider all feasible paths for reverse path verification and only active path based verification is supported.
- uRPF failure packets statistics are not supported in ACX.
- You can use either the `show interfaces extensive` command or the `show interfaces detail` command to verify that unicast RPF is enabled and working on the interface. In the Flags section of the output, if unicast reverse-path forwarding (RPF) is explicitly configured on the specified interface, the uRPF flag is displayed. If unicast RPF was configured on a different interface (and therefore is enabled on all switch interfaces) but was not explicitly configured on the specified interface, the uRPF flag is not displayed even though unicast RPF is enabled.
- The uRPF detail in the Flags section of the output of the `show interfaces (detail | extensive)` commands is displayed only for logical interfaces on which uRPF is configured. Otherwise, this information is not shown.

Related Documentation

Understanding Unicast RPF (Routers)

For interfaces that carry IPv4 or IPv6 traffic, you can reduce the impact of denial of service (DoS) attacks by configuring unicast reverse path forwarding (RPF). Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.
NOTE:

- You can protect a network by applying unicast RPF check feature at the edge (on customer facing interfaces) of the network. In an ISP environment, this can impact the network which can impose on a scaled setup. In case if you have already protected the edge of your network, a packet with a spoofed IP source address would not even appear in a core facing interface. In this case, unicast RPF check is not necessary. Enabling unicast RPF feature can impact the control plane performance, so use it where it is required. So it is strongly recommended not to enable this feature on the network core (internal) interfaces.

- Unicast RPF and Default Route on page 227
- Configuring Unicast RPF Strict Mode on page 229
- Configuring Unicast RPF Loose Mode on page 231
- Configuring Unicast RPF Loose Mode with Ability to Discard Packets on page 233
- Configuring Unicast RPF on a VPN on page 234
- Configuring Unicast RPF on page 235

**Unicast RPF and Default Route**

When the active route cannot be chosen from the routes in a routing table, the router chooses a default route. A default route is equivalent to an IP address of 0.0.0.0/0. If you configure a default route, and you configure unicast RPF on an interface that the default route uses, unicast RPF behaves differently than it does otherwise. For information about configuring default routes, see the *Junos OS Routing Protocols Library*.

To determine whether the default route uses an interface, enter the `show route` command:

```
user@host> show route address
```

*address* is the next-hop address of the configured default route. The default route uses the interfaces shown in the output of the `show route` command.

The following sections describe how unicast RPF behaves when a default route uses an interface and when a default route does not use an interface:

- Unicast RPF Behavior with a Default Route on page 228
- Unicast RPF Behavior Without a Default Route on page 228
- Unicast RPF with Routing Asymmetry on page 229
### Unicast RPF Behavior with a Default Route

On all routers except those with MPCs and the MX80 router, unicast RPF behaves as follows if you configure a default route that uses an interface configured with unicast RPF:

- **Loose mode**—All packets are automatically accepted. For this reason, we recommend that you not configure unicast RPF loose mode on interfaces that the default route uses.
- **Strict mode**—The packet is accepted when the source address of the packet matches any of the routes (either default or learned) that can be reached through the interface. Note that routes can have multiple destinations associated with them; therefore, if one of the destinations matches the incoming interface of the packet, the packet is accepted.

On all routers with MPCs and the MX80 router, unicast RPF behaves as follows if you configure a default route that uses an interface configured with unicast RPF:

- **Loose mode**—All packets except the packets whose source is learned from the default route are accepted. All packets whose source is learned from the default route are dropped at the Packet Forwarding Engine. The default route is treated as if the route does not exist.
- **Strict mode**—The packet is accepted when the source address of the packet matches any of the routes (either default or learned) that can be reached through the interface. Note that routes can have multiple destinations associated with them; therefore, if one of the destinations matches the incoming interface of the packet, the packet is accepted.

On all routers, the packet is not accepted when either of the following is true:

- The source address of the packet does not match a prefix in the routing table.
- The interface does not expect to receive a packet with this source address prefix.

### Unicast RPF Behavior Without a Default Route

If you do not configure a default route, or if the default route does not use an interface configured with unicast RPF, unicast RPF behaves as described in “Configuring Unicast RPF Strict Mode” on page 229 and “Configuring Unicast RPF Loose Mode” on page 231. To summarize, unicast RPF without a default route behaves as follows:

- **Strict mode**—The packet is not accepted when either of the following is true:
  - The packet has a source address that does not match a prefix in the routing table.
  - The interface does not expect to receive a packet with this source address prefix.
- **Loose mode**—The packet is not accepted when the packet has a source address that does not match a prefix in the routing table.
Unicast RPF with Routing Asymmetry

In general, we recommend that you not enable unicast RPF on interfaces that are internal to the network because internal interfaces are likely to have routing asymmetry. Routing asymmetry means that a packet’s outgoing and return paths are different. Routers in the core of the network are more likely to have asymmetric reverse paths than routers at the customer or provider edge. Figure 12 on page 229 shows unicast RPF in an environment with routing asymmetry.

Figure 12: Unicast RPF with Routing Asymmetry

In Figure 12 on page 229, if you enable unicast RPF on interface so-0/0/0, traffic destined for Router A is not rejected. If you enable unicast RPF on interface so-1/0/1, traffic from Router A is rejected.

If you need to enable unicast RPF in an asymmetric routing environment, you can use fail filters to allow the router to accept incoming packets that are known to be arriving by specific paths. For an example of a fail filter that accepts packets with a specific source and destination address, see “Configuring Unicast RPF” on page 235.

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

If the incoming packet fails the unicast RPF check, the packet is not accepted on the interface. When a packet is not accepted on an interface, unicast RPF counts the packet and sends it to an optional fail filter. If the fail filter is not configured, the default action is to silently discard the packet.

The optional fail filter allows you to apply a filter to packets that fail the unicast RPF check. You can define the fail filter to perform any filter operation, including accepting, rejecting, logging, sampling, or policing.

When unicast RPF is enabled on an interface, Bootstrap Protocol (BOOTP) packets and Dynamic Host Configuration Protocol (DHCP) packets are not accepted on the interface. To allow the interface to accept BOOTP packets and DHCP packets, you must apply a fail filter that accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255. For a configuration example, see “Configuring Unicast RPF” on page 235.

For more information about unicast RPF, see the Junos OS Routing Protocols Library. For more information about defining fail filters, see the Routing Policies, Firewall Filters, and Traffic Policers Feature Guide.
To configure unicast RPF, include the `rpf-check` statement:

```
rpf-check <fail-filter filter-name>;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family (inet | inet6)]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (inet | inet6)]`

Using unicast RPF can have several consequences when implemented with traffic filters:

- RPF fail filters are evaluated after input filters and before output filters.
- If you configure a filter counter for packets dropped by an input filter, and you want to know the total number of packets dropped, you must also configure a filter counter for packets dropped by the RPF check.
- To count packets that fail the RPF check and are accepted by the RPF fail filter, you must configure a filter counter.
- If an input filter forwards packets anywhere other than the inet.0 or inet6.0 routing tables, the unicast RPF check is not performed.
- If an input filter forwards packets anywhere other than the routing instance the input interface is configured for, the unicast RPF check is not performed.

Configure unicast RPF strict mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of `0.0.0.0` and a destination address of `255.255.255.255`.

To configure unicast RPF in strict mode:

1. Configure the fail filter:

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
    term allow-dhcp-bootp {
        from {
            source-address {
                0.0.0.0/32;
            } address {
                255.255.255.255/32;
            }
        }
        then {
            count rpf-dhcp-bootp-traffic;
            accept;
        }
    }
    term default {
        then {
            log;
        }
    }
}
```
2. Configure unicast RPF on interfaces:

```plaintext
[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
      }
    }
  }
}
```

3. Commit the configuration.

```plaintext
[edit]
commit;
```

Configuring Unicast RPF Loose Mode

By default, unicast RPF uses strict mode. Unicast RPF loose mode is similar to unicast RPF strict mode and has the same configuration restrictions. The only check in loose mode is whether the packet has a source address with a corresponding prefix in the routing table; loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. If a corresponding prefix is not found, unicast RPF loose mode does not accept the packet. As in strict mode, loose mode counts the failed packet and optionally forwards it to a fail filter, which either accepts, rejects, logs, samples, or polices the packet.

To configure unicast RPF loose mode, include the `mode`:

1. `mode loose;`

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family (inet | inet6) rpf-check <fail-filter filter-name>]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (inet | inet6) rpf-check <fail-filter filter-name>]`

2. For example:

   In this example, no special configuration beyond device initialization is required.
Configure unicast RPF loose mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of **0.0.0.0** and a destination address of **255.255.255.255**.

To configure unicast RPF in loose mode:

a. Configure the fail filter:

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
    term allow-dhcp-bootp {
        from {
            source-address {
                0.0.0.0/32;
            }
            address {
                255.255.255.255/32;
            }
        }
        then {
            count rpf-dhcp-bootp-traffic;
            accept;
        }
    }
    term default {
        then {
            log;
            reject;
        }
    }
}
```

b. Configure unicast RPF on interfaces:

```
[edit]
interfaces {
    so-0/0/0 {
        unit 0 {
            family inet {
                rpf-check fail-filter rpf-special-case-dhcp-bootp;
                mode loose;
            }
        }
    }
}
```

c. Commit the configuration.

```
[edit]
commit;
```
Configuring Unicast RPF Loose Mode with Ability to Discard Packets

Starting with Junos OS Release 12.1, unicast RPF loose mode has the ability to discard packets with the source address pointing to the discard interface. This feature is supported on MX Series routers and on T Series routers with Type 1 FPCs, Type 2 FPCs, and Type 3 FPCs. Using unicast RPF loose mode, along with Remote Triggered Black Hole (RTBH) filtering, provides an efficient way to discard packets coming from known attack sources. BGP policies in edge routers ensure that packets with untrusted source addresses have their next hop set to a discard route. When a packet arrives at the router with an untrusted source address, unicast RPF performs a route lookup of the source address. Because the source address route points to a discard next hop, the packet is dropped and a counter is incremented. This feature is supported on both IPv4 (inet) and IPv6 (inet6) address families.

To configure unicast RPF loose mode with the ability to discard packets, include the `rpf-loose-mode-discard family inet` statement at the [edit forwarding-options] hierarchy level:

```
rpf-loose-mode-discard {
    family {
        inet;
    }
}
```

In this example, no special configuration beyond device initialization is required.

Configure unicast RPF loose mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

To configure unicast RPF loose mode with the ability to discard packets:

1. **Configure the fail filter:**

   ```
   [edit firewall]
   filter rpf-special-case-dhcp-bootp {
     term allow-dhcp-bootp {
       from {
         source-address {
           0.0.0.0/32;
         }
         address {
           255.255.255.255/32;
         }
       }
       then {
         count rpf-dhcp-bootp-traffic;
         accept;
       }
     }
     term default {
       then {
   ```
2. Configure unicast RPF on interfaces:

```
[edit]
interfaces {  
  so-0/0/0 {  
    unit 0 {  
      family inet {  
        rpf-check fail-filter rpf-special-case-dhcp-bootp;  
        mode loose;  
        }  
      }  
    }  
  }  
}
```

3. Configure the ability to discard packets.

```
[edit]
forwarding-options{  
  rpf-loose-mode-discard {  
    family {  
      inet;  
    }  
  }  
}
```

4. Commit the configuration.

```
[edit]
commit;
```

Configuring Unicast RPF on a VPN

You can configure unicast RPF on a VPN interface by enabling unicast RPF on the interface and including the `interface` statement at the `[edit routing-instances routing-instance-name]` hierarchy level.

You can configure unicast RPF only on the interfaces you specify in the routing instance. This means the following:

- For Layer 3 VPNs, unicast RPF is supported on the CE router interface.
- Unicast RPF is not supported on core-facing interfaces.
For virtual-router routing instances, unicast RPF is supported on all interfaces you specify in the routing instance.

If an input filter forwards packets anywhere other than the routing instance the input interface is configured for, the unicast RPF check is not performed.

For more information about VPNS and virtual-router routing instances, see the Junos OS VPNs Library for Routing Devices. For more information about FBF, see the Junos OS Routing Protocols Library.

Configure unicast RPF on a Layer 3 VPN interface:

```
[edit interfaces]
so-0/0/0 {
  unit 0 {
    family inet {
      rpf-check;
    }
  }
}
[edit routing-instance]
VPN-A {
  interface so-0/0/0;
}
```

**Configuring Unicast RPF**

Configure unicast RPF strict mode, and apply a fail filter that allows the interface to accept BOOTP packets and DHCP packets. The filter accepts all packets with a source address of 0.0.0.0 and a destination address of 255.255.255.255.

```
[edit firewall]
filter rpf-special-case-dhcp-bootp {
  term allow-dhcp-bootp {
    from {
      source-address {
        0.0.0.0/32;
      }
      address {
        255.255.255.255/32;
      }
    }
    then {
      count rpf-dhcp-bootp-traffic;
      accept;
    }
  }
  term default {
    then {
      log;
      reject;
    }
  }
}
```
[edit]
interfaces {
  so-0/0/0 {
    unit 0 {
      family inet {
        rpf-check fail-filter rpf-special-case-dhcp-bootp;
      }
    }
  }
}

See Also  •  unicast-reverse-path

Understanding and Preventing Unknown Unicast Forwarding

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that traverse a VLAN to all interfaces that are members of that VLAN. Forwarding this type of traffic can create unnecessary traffic that leads to poor network performance or even a complete loss of network service. This flooding of packets is known as a traffic storm.

To prevent a traffic storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring specific VLANs or all VLANs to forward all unknown unicast traffic traversing them to a specific interface. You can configure multiple VLANs to forward unknown unicast packets to the same interface or configure different interfaces for different VLANs. This channels the unknown unicast traffic traversing VLANs to specific interfaces instead of flooding all interfaces.

•  Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface on page 236
•  Configuring Unknown Unicast Forwarding (ELS) on page 237
•  Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 240
•  Configuring Unknown Unicast Forwarding (CLI Procedure) on page 241

Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface

Purpose  Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single interface instead of flooding unknown unicast packets across all interfaces that are members of that VLAN.

NOTE:  This procedure 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: “Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface” on page 240. For ELS details see: Using the Enhanced Layer 2 Software CLI.
**Action**  
(EX4300 Switches) Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

```
user@switch> show configuration switch-options

unknown-unicast-forwarding {
  vlan v1 {
    interface ge-0/0/7.0;
  }
}
```

(EX9200 Switches) Display the forwarding interface for unknown unicast packets:

```
user@switch> show forwarding-options

next-hop-group uuf-nhg {
  group-type layer-2;
  interface ge-0/0/7.0;
}
```

**Meaning**  
The sample output from the `show` commands show that the unknown unicast forwarding interface for VLAN v1 is interface `ge-0/0/7`.

**Configuring Unknown Unicast Forwarding (ELS)**

![NOTE:](image)

**NOTE:** This task uses Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style. If your EX Series switch runs software that does not support ELS, see “Configuring Unknown Unicast Forwarding (CLI Procedure)” on page 241. For ELS details, see Using the Enhanced Layer 2 Software CLI

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets that traverse a VLAN to all interfaces associated with that VLAN. This flooding of packets is known as a traffic storm and can negatively impact network performance.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN to a specific interface. You can configure each VLAN to divert unknown unicast traffic to a different interface or use the same interface for multiple VLANs.

- Configuring Unknown Unicast Forwarding on EX4300 Switches on page 238
- Configuring Unknown Unicast Forwarding on EX9200 Switches on page 238
Configuring Unknown Unicast Forwarding on EX4300 Switches

To configure unknown unicast forwarding options on EX4300 switches:

- Configure unknown unicast forwarding for a specific VLAN and specify the interface to which all unknown unicast traffic will be forwarded:

  ```
  [edit switch-options]
  user@switch# set unknown-unicast-forwarding vlan vlan-name interface interface-name
  ```

- Configure unknown unicast forwarding for all VLANs and specify the interface to which all unknown unicast traffic will be forwarded:

  ```
  [edit switch-options]
  user@switch# set unknown-unicast-forwarding vlan all interface interface-name
  ```

Configuring Unknown Unicast Forwarding on EX9200 Switches

To configure unknown unicast forwarding on EX9200 switches, you must configure a flood filter and apply it to VLANs for which you want to configure unknown unicast forwarding. Flood filters are firewall filters that are applied only to broadcast, unknown unicast, and multicast (BUM) traffic. If a flood filter is configured, only traffic packets that are of the packet type unknown-unicast are forwarded to the interface on which unicast forwarding is configured. A next-hop group redirects the packets according to the action specified in the flood filter.

To configure the next-hop group that receives Layer 2 packets and then configure the interface to which these packets are forwarded:

1. Configure the `next-hop-group` action for the Layer 2 interface expected to receive unknown unicast packets:

   ```
   [edit forwarding-options]
   user@switch# set next-hop-group next-hop-group-name group-type layer-2
   [edit forwarding-options]
   user@switch# set next-hop-group next-hop-group-name interface interface-name
   ```

   For example:

   ```
   [edit forwarding-options]
   user@switch# set next-hop-group uuf-nhg group-type layer-2
   [edit forwarding-options]
   user@switch# set next-hop-group uuf-nhg interface ge-3/1/7.0
   ```

2. Configure a firewall filter with family address type `ethernet-switching`:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter filter-name
   ```

   For example:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter uuf_filter
   ```
3. Configure a term in the firewall filter for the interface that receives unknown unicast packets (the interface specified in Step 1) to discard unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from interface interface-name
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then discard
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term source-drop from interface ge-3/1/7.0
user@switch# set term source-drop from traffic-type unknown-unicast
user@switch# set term source-drop then discard
```

4. Configure a term in the firewall filter for unknown unicast packets to be flooded to the interface enabled for unknown unicast forwarding by using `next-hop-group` (in step 1):

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then next-hop-group group-name
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term uuf-flood from traffic-type unknown-unicast
user@switch# set term uuf-flood then next-hop-group uuf-nhg
```

5. Configure a default term for the firewall filter to forward packets other than unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name then accept
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term fwd-default then accept
```

6. Apply the filter as a flood filter on the VLAN that includes the interface which will receive unknown unicast packets:

```
[edit vlans vlan-name]
user@switch# set forwarding-options flood input filter-name
```

For example:

```
[edit vlans v1]
user@switch# set forwarding-options flood input uuf_filter
```
Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface

**Purpose**  Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single trunk interface instead of flooding unknown unicast packets across all interfaces that are members of the same VLAN.

**Action**  Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

```
user@switch> show configuration ethernet-switching-options
unknown-unicast-forwarding {
    vlan v1 {
        interface ge-0/0/7.0;
    }
}
```

Display the Ethernet switching table:

```
user@switch> show ethernet-switching table vlan v1
Ethernet-switching table: 3 unicast 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>v1</td>
<td>*</td>
<td>Flood</td>
<td></td>
<td>All-members</td>
</tr>
<tr>
<td>v1</td>
<td>00:01:09:00:00:00</td>
<td>Learn</td>
<td>24</td>
<td>ge-0/0/7.0</td>
</tr>
<tr>
<td>v1</td>
<td>00:11:09:00:01:00</td>
<td>Learn</td>
<td>37</td>
<td>ge-0/0/3.0</td>
</tr>
</tbody>
</table>
```

**Meaning**  The sample output from the `show configuration ethernet-switching-options` command shows that the unknown unicast forwarding interface for VLAN v1 is interface `ge-0/0/7`. The `show ethernet-switching table` command shows that an unknown unicast packet is received on interface `ge-0/0/3` with the destination MAC address (DMAC) `00:01:09:00:00:00` and the source MAC address (SMAC) of `00:11:09:00:01:00`. This shows that the SMAC of the packet is learned in the normal way (through the interface `ge-0/0/3.0`), while the DMAC is learned on interface `ge-0/0/7`.

**See Also**
Configuring Unknown Unicast Forwarding (CLI Procedure)

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific trunk interface. From there, the destination MAC address can be learned and added to the Ethernet switching table. You can configure each VLAN to divert unknown unicast traffic to different trunk interfaces or use one trunk interface for multiple VLANs.

NOTE: For Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style, see “Configuring Unknown Unicast Forwarding (ELS)” on page 237.

To configure unknown unicast forwarding options:

NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

1. Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is employee):

   ```
   [edit ethernet-switching-options]
   user@switch# set unknown-unicast-forwarding vlan employee
   ```

2. Specify the trunk interface to which all unknown unicast traffic will be forwarded:

   ```
   [edit ethernet-switching-options]
   user@switch# set unknown-unicast-forwarding vlan employee interface ge-0/0/3.0
   ```

Related Documentation

- Understanding and Preventing Unknown Unicast Forwarding on page 236
- Understanding Storm Control
- Configuring Autorecovery for Port Security Events

Enabling Source Class and Destination Class Usage

- Source Class and Destination Class Usage on page 241
- Enabling Source Class and Destination Class Usage on page 245

Source Class and Destination Class Usage

For interfaces that carry IPv4, IPv6, MPLS, or peer AS billing traffic, you can maintain packet counts based on the entry and exit points for traffic passing through your network.
Entry and exit points are identified by source and destination prefixes grouped into disjoint sets defined as source classes and destination classes. You can define classes based on a variety of parameters, such as routing neighbors, autonomous systems, and route filters.

Source class usage (SCU) counts packets sent to customers by performing lookup on the IP source address. SCU makes it possible to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. You must enable SCU accounting on both the inbound and outbound physical interfaces, and the route for the source of the packet must be in located in the forwarding table.

**NOTE:** SCU and DCU accounting do not work with directly connected interface routes. Source class usage does not count packets coming from sources with direct routes in the forwarding table because of software architecture limitations.

Destination class usage (DCU) counts packets from customers by performing lookup of the IP destination address. DCU makes it possible to track traffic originating from the customer edge and destined for specific prefixes on the provider core router.

**NOTE:** We recommend that you stop the network traffic on an interface before you modify the DCU or SCU configuration for that interface. Modifying the DCU or SCU configuration without stopping the traffic might corrupt the DCU or SCU statistics. Before you restart the traffic after modifying the configuration, enter the clear interfaces statistics command.

Figure 13 on page 242 illustrates an Internet service provider (ISP) network. In this topology, you can use DCU to count packets customers send to specific prefixes. For example, you can have three counters, one per customer, that count the packets destined for prefix 210.210/16 and 220.220/16.

You can use SCU to count packets the provider sends from specific prefixes. For example, you can count the packets sent from prefix 210.210/16 and 215.215/16 and transmitted on a specific output interface.

*Figure 13: Prefix Accounting with Source and Destination Classes*
You can configure up to 126 source classes and 126 destination classes. For each interface on which you enable destination class usage and source class usage, the Junos OS maintains an interface-specific counter for each corresponding class up to the 126 class limit.

**NOTE:** For transit packets exiting the router through the tunnel, forwarding path features, such as RPF, forwarding table filtering, source class usage, and destination class usage are not supported on the interfaces you configure as the output interface for tunnel traffic. For firewall filtering, you must allow the output tunnel packets through the firewall filter applied to input traffic on the interface that is the next-hop interface towards the tunnel destination.

**NOTE:**
Performing DCU accounting when an output service is enabled produces inconsistent behavior in the following configuration:

- Both SCU input and DCU are configured on the packet input interface.
- SCU output is configured on the packet output interface.
- Interface services is enabled on the output interface.

For an incoming packet with source and destination prefixes matching the SCU and DCU classes respectively configured in the router, both SCU and DCU counters will be incremented. This behavior is not harmful or negative. However, it is inconsistent with non-serviced packets, in that only the SCU count will be incremented (because the SCU class ID will override the DCU class ID in this case).

To enable packet counting on an interface, include the `accounting` statement:

```
accounting {
    destination-class-usage;
    source-class-usage {
        direction;
    }
}
```

`direction` can be one of the following:

- **input**—Configure at least one expected ingress point.
- **output**—Configure at least one expected egress point.
- **input output**—On a single interface, configure at least one expected ingress point and one expected egress point.

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family (inet | inet6 | mpls)]`
• \texttt{[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family \{inet | inet6 | mpls\}]} For SCU to work, you must configure at least one input interface and at least one output interface.

The ability to count a single packet for both SCU and DCU accounting depends on the underlying physical interface.

• For traffic over MPC/MIC interfaces, a single incoming packet is counted for both SCU and DCU accounting if both SCU and DCU are configured. To ensure the outgoing packet is counted, include the \texttt{source-class-usage output} statements in the configuration of the outgoing interface.

• For traffic over DPC interfaces, an incoming packet is counted only once, and SCU takes priority over DCU. This means that when a packet arrives on an interface on which you include the \texttt{source-class-usage input} and \texttt{destination-class-usage} statements in the configuration, and when the source and destination both match accounting prefixes, the Junos OS associates the packet with the source class only.

For traffic over MPC interfaces, SCU and DCU accounting is performed after output filters are evaluated. If a packet matches a firewall filter match condition, the packet is included in SCU or DCU accounting except in the case where the action of the matched term is \texttt{discard}.

On T Series, M120, and M320 routers, the source class and destination classes are not carried across the router fabric. The implications of this are as follows:

• On T Series, M120, and M320 routers, SCU and DCU accounting is performed before the packet enters the fabric.

• On M7i, M10i, M120, and M320 routers, on MX Series routers with non-MPC, and on T Series routers, SCU and DCU accounting is performed before output filters are evaluated. Consequently, if a packet matches a firewall filter match condition, the packet is included in SCU or DCU accounting; the packet is counted for any term action (including the \texttt{discard} action).

• On M120, M320, and T Series routers, the \texttt{destination-class} and \texttt{source-class} statements are supported at the \texttt{[edit firewall family family-name filter filter-name term term-name from]} hierarchy level only for the filter applied to the forwarding table. On M7i, M10i, and MX Series routers, these statements are supported.

Once you enable accounting on an interface, the Junos OS maintains packet counters for that interface, with separate counters for \texttt{inet}, \texttt{inet6}, and \texttt{mpls} protocol families. You must then configure the source class and destination class attributes in policy action statements, which must be included in forwarding-table export policies.

\textbf{NOTE:} When configuring policy action statements, you can configure only one source class for each matching route. In other words, more than one source class cannot be applied to the same route.
In Junos OS Release 9.3 and later, you can configure SCU accounting for Layer 3 VPNs configured with the \texttt{vrf-table-label} statement. Include the \texttt{source-class-usage} statement at the \texttt{[edit routing-instances routing-instance-name vrf-table-label]} hierarchy level. The \texttt{source-class-usage} statement at this hierarchy level is supported only for the virtual routing and forwarding (VRF) instance type.

**NOTE:** DCU counters cannot be enabled on the label-switched interface (LSI) that is created dynamically when the \texttt{vrf-table-label} statement is configured within a VRF. For more information, see the Junos OS VPNs Library for Routing Devices.

For a complete discussion about source and destination class accounting profiles, see the Network Management and Monitoring Guide. For more information about MPLS, see the MPLS Applications Feature Guide.

### Enabling Source Class and Destination Class Usage

**Figure 14: Prefix Accounting with Source and Destination Classes**

Configure DCU and SCU output on one interface:

```plaintext
[edit]
interfaces {
  so-6/1/0 {
    unit 0 {
      family inet {
        accounting {
          destination-class-usage;
          source-class-usage {
            output;
          }
        }
        SCU output /DCU
      }
    }
  }
}
```
1. Source routers A and B use loopback addresses as the prefixes to be monitored. Most of the configuration tasks and actual monitoring occur on transit Router SCU.

The loopback address on Router A contains the origin of the prefix that is to be assigned to source class A on Router SCU. However, no SCU processing happens on this router. Therefore, configure Router A for basic OSPF routing and include your loopback interface and interface so-0/0/2 in the OSPF process.

2. 

```diff
[edit]
interfaces {
    so-0/0/2 {
        unit 0 {
            family inet {
                address 10.255.50.2/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.255.192.10/32;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/2.0;
            interface lo0.0;
        }
    }
}
```

3. Last, apply the policy to the forwarding table.

Router SCU handles the bulk of the activity in this example. On Router SCU, enable source class usage on the inbound and outbound interfaces at the [edit interfaces interface-name unit unit-number family inet accounting] hierarchy level. Make sure you specify the expected traffic: input, output, or, in this case, both.

Next, configure a route filter policy statement that matches the prefixes of the loopback addresses from routers A and B. Include statements in the policy that classify packets from Router A in one group named scu-class-a and packets from Router B in a second class named scu-class-b. Notice the efficient use of a single policy containing multiple terms.

```diff
[edit]
interfaces {
    scu-class-a {
        route-filter apply;
    }
    scu-class-b {
        route-filter apply;
    }
```
so-0/0/1 {
  unit 0 {
    family inet {
      accounting {
        source-class-usage {
          input;
          output;
        }
        address 10.255.50.1/24;
      }
    }
  }
}

so-0/0/3 {
  unit 0 {
    family inet {
      accounting {
        source-class-usage {
          input;
          output;
        }
        address 10.255.10.3/24;
      }
    }
  }
}

lo0 {
  unit 0 {
    family inet {
      address 10.255.6.111/32;
    }
  }
}

protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/1.0;
      interface so-0/0/3.0;
    }
  }
}

routing-options {
  forwarding-table {
    export scu-policy;
  }
}

policy-options {
  policy-statement scu-policy {
    term 0 {
      from {
        route-filter 10.255.192.0/24 orlonger;
      }
      then source-class scu-class-a;
    }
  }
}
4. Just as Router A provides a source prefix, Router B's loopback address matches the prefix assigned to \texttt{scu-class-b} on Router SCU. Again, no SCU processing happens on this router, so configure Router B for basic OSPF routing and include your loopback interface and interface \texttt{so-0/0/4} in the OSPF process.

```bash
interfaces {
    so-0/0/4 {
        unit 0 {
            family inet {
                address 10.255.10.4/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.255.165.226/32;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

5. You can use SCU and DCU to count packets on Layer 3 VPNs. To enable packet counting for Layer 3 VPN implementations at the egress point of the MPLS tunnel, you must configure a virtual loopback tunnel interface (vt) on the PE router, map the virtual routing and forwarding (VRF) instance type to the virtual loopback tunnel interface, and send the traffic received from the VPN out the source class output interface, as shown in the following example:

Configure a virtual loopback tunnel interface on a provider edge router equipped with a tunnel PIC:

```bash
[edit interfaces]
vt-0/3/0 {
    unit 0 {
```
6. Map the VRF instance type to the virtual loopback tunnel interface.

In Junos OS Release 9.3 and later, you can configure SCU accounting for Layer 3 VPNs configured with the `vrf-table-label` statement. Include the `source-class-usage` statement at the `[edit routing-instances routing-instance-name vrf-table-label]` hierarchy level. The `source-class-usage` statement at this hierarchy level is supported only for the virtual routing and forwarding (VRF) instance type. DCU is not supported when the `vrf-table-label` statement is configured. For more information, see the Junos OS VPNs Library for Routing Devices.

   [edit routing-instances]
   VPN-A {
      instance-type vrf;
      interface at-2/1/1.0;
      interface vt-0/3/0.0;
      route-distinguisher 10.255.14.225:100;
      vrf-import import-policy-A;
      vrf-export export-policy-A;
      protocols {
         bgp {
            group to-r4 {
               local-address 10.27.253.1;
               peer-as 400;
               neighbor 10.27.253.2;
            }
         }
      }
   }

7. Send traffic received from the VPN out the source class output interface:

   [edit interfaces]
   at-2/1/0 {
      unit 0 {
         family inet {
            accounting {
               source-class-usage {
                  output;
               }
            }
         }
      }
   }

Targeted broadcast is a process of flooding a target subnet with Layer 3 broadcast IP packets originating from a different subnet. The intent of targeted broadcast is to flood the target subnet with the broadcast packets on a LAN interface without broadcasting to the entire network. Targeted broadcast is configured with various options on the egress interface of the router or switch and the IP packets are broadcast only on the LAN (egress) interface. Targeted broadcast helps you implement remote administration tasks such as backups and wake-on LAN (WOL) on a LAN interface, and supports virtual routing and forwarding (VRF) instances.

Regular Layer 3 broadcast IP packets originating from a subnet are broadcast within the same subnet. When these IP packets reach a different subnet, they are forwarded to the Routing Engine (to be forwarded to other applications). Because of this, remote administration tasks such as backups cannot be performed on a particular subnet through another subnet. As a workaround you can enable targeted broadcast, to forward broadcast packets that originate from a different subnet.

Layer 3 broadcast IP packets have a destination IP address that is a valid broadcast address for the target subnet. These IP packets traverse the network in the same way as unicast IP packets until they reach the destination subnet. In the destination subnet, if the receiving router has targeted broadcast enabled on the egress interface, the IP packets are forwarded to an egress interface and the Routing Engine or to an egress interface only. The IP packets are then translated into broadcast IP packets which flood the target subnet only through the LAN interface (if there is no LAN interface, the packets are discarded), and all hosts on the target subnet receive the IP packets. If targeted broadcast is not enabled on the receiving router, the IP packets are treated as regular Layer 3 broadcast IP packets and are forwarded to the Routing Engine. If targeted broadcast is enabled without any options, the IP packets are forwarded to the Routing Engine.
Targeted broadcast can be configured to forward the IP packets only to an egress interface, which is helpful when the router is flooded with packets to process, or to both an egress interface and the Routing Engine.

**NOTE:** Targeted broadcast does not work when the targeted broadcast option forward-and-send-to-re and the traffic sampling option sampling are configured on the same egress interface of an M320 router, a T640 router, or an MX960 router. To overcome this scenario, you must either disable one of the these options or enable the sampling option with the targeted broadcast option forward-only on the egress interface. For information about traffic sampling, see Configuring Traffic Sampling.

**NOTE:** Any firewall filter that is configured on the Routing Engine loopback interface (lo0) cannot be applied to IP packets that are forwarded to the Routing Engine as a result of a targeted broadcast. This is because broadcast packets are forwarded as flood next hop and not as local next hop traffic, and you can only apply a firewall filter to local next hop routes for traffic directed towards the Routing Engine.

**Related Documentation**

- targeted-broadcast on page 1044

## Configuring Targeted Broadcast

The following sections explain how to configure targeted broadcast on an egress interface and its options:

- Configuring Targeted Broadcast and Its Options on page 251
- Display Targeted Broadcast Configuration Options on page 252

### Configuring Targeted Broadcast and Its Options

You can configure targeted broadcast on an egress interface with different options. You can either allow the IP packets destined for a Layer 3 broadcast address to be forwarded on the egress interface and to send a copy of the IP packets to the Routing Engine or you can allow the IP packets to be forwarded on the egress interface only. Note that the packets are broadcast only if the egress interface is a LAN interface.

To configure targeted broadcast and its options:

1. Configure the physical interface.

   ```
   [edit]
   user@host# set interfaces interface-name
   ```

2. Configure the logical unit number at the [edit interfaces interface-name] hierarchy level.
[edit interfaces interface-name]
user@host# set unit logical-unit-number

3. Configure the protocol family as inet at the [edit interfaces interface-name unit interface-unit-number] hierarchy level.

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

4. Configure targeted broadcast at the [edit interfaces interface-name unit interface-unit-number family inet] hierarchy level

[edit interfaces interface-name unit interface-unit-number family inet]
user@host# set targeted-broadcast

5. Specify one of the following options as per requirement:
   • To allow IP packets destined for a Layer 3 broadcast address to be forwarded on the egress interface and to send a copy of the IP packets to the Routing Engine.
     [edit interfaces interface-name unit interface-unit-number family inet targeted-broadcast]
     user@host# set forward-and-send-to-re
   • To allow IP packets to be forwarded on the egress interface only.
     [edit interfaces interface-name unit interface-unit-number family inet targeted-broadcast]
     user@host# set forward-only

---

NOTE: Targeted broadcast does not work when the targeted broadcast option forward-and-send-to-re and the traffic sampling option sampling are configured on the same egress interface of an M320 router, a T640 router, or an MX960 router. To overcome this scenario, you must either disable one of the these options or enable the sampling option with the targeted broadcast option forward-only on the egress interface. For information about traffic sampling, see Configuring Traffic Sampling.

---

Display Targeted Broadcast Configuration Options

The following topics display targeted broadcast configuration with its various options:

• Forward IP Packets On the Egress Interface and To the Routing Engine on page 253
• Forward IP Packets On the Egress Interface Only on page 253
Forward IP Packets On the Egress Interface and To the Routing Engine

**Purpose**
Display the configuration when targeted broadcast is configured on the egress interface to forward the IP packets on the egress interface and to send a copy of the IP packets to the Routing Engine.

**Action**
To display the configuration run the `show` command at the `[edit interfaces interface-name unit interface-unit-number family inet]` where the interface name is ge-2/0/0, the unit value is set to 0, the protocol family is set to inet.

```plaintext
[edit interfaces interface-name unit interface-unit-number family inet]
user@host#show
    targeted-broadcast {
        forward-and-send-to-re;
    }
```

Forward IP Packets On the Egress Interface Only

**Purpose**
Display the configuration when targeted broadcast is configured on the egress interface to forward the IP packets on the egress interface only.

**Action**
To display the configuration run the `show` command at the `[edit interfaces interface-name unit interface-unit-number family inet]` where the interface name is ge-2/0/0, the unit value is set to 0, the protocol family is set to inet.

```plaintext
[edit interfaces interface-name unit interface-unit-number family inet]
user@host#show
    targeted-broadcast {
        forward-only;
    }
```

**Related Documentation**
- targeted-broadcast on page 1044
CHAPTER 5

Configuring Circuit and Translational Cross-Connects

- Circuit and Translational Cross-Connects Overview on page 255
- Defining the Encapsulation for Switching Cross-Connects on page 257
- Defining the Connection for Switching Cross-Connects on page 261
- Configuring MPLS for Switching Cross-Connects on page 261
- Configuring IS-IS or MPLS Traffic for TCC Interfaces on page 262
- Configuring ATM-to-Ethernet Interworking on page 262
- ATM-To-Ethernet Interworking on ATM MICs on page 267
- Example: Configuring a CCC over Frame Relay Encapsulated Interface on page 268
- Example: Configuring a TCC on page 269
- Example: Configuring CCC over Aggregated Ethernet on page 270
- Example: Configuring a Remote LSP CCC over Aggregated Ethernet on page 272
- Example: Configuring ATM-to-Ethernet Interworking on page 274
- Example: Configuring ATM-to-Ethernet Interworking on ATM MIC on page 275
- Verifying ATM-to-Ethernet Interworking Configuration on ATM MICs on page 281

Circuit and Translational Cross-Connects Overview

Circuit cross-connect (CCC) and translational cross-connect (TCC) allow you to configure transparent connections between two circuits, where a circuit can be a Frame Relay data-link connection identifier (DLCI), an Asynchronous Transfer Mode (ATM) virtual circuit (VC), a Point-to-Point Protocol (PPP) interface, a Cisco High-level Data Link Control (HDLC) interface, or a Multiprotocol Label Switching (MPLS) label-switched path (LSP).

Using CCC or TCC, packets from the source circuit are delivered to the destination circuit with, at most, the Layer 2 address being changed. No other processing, such as header checksums, time-to-live (TTL) decrementing, or protocol processing, is done.

To connect interfaces of the same type, use CCC. To connect unlike interfaces, use TCC.
CCC and TCC circuits fall into three categories: logical interfaces, which include ATM VCs and Frame Relay DLCIs; physical interfaces, which include PPP and Cisco HDLC; and paths, which include LSPs. The three circuit categories provide three types of cross-connect:

- **Layer 2 switching (interface-to-interface)**—Cross-connects between logical interfaces provide what is essentially Layer 2 switching.
- **MPLS tunneling (interface-to-LSP)**—Cross-connects between interfaces and LSPs allow you to connect two distant interface circuits by creating MPLS tunnels that use LSPs as the conduit.
- **LSP stitching (LSP-to-LSP)**—Cross-connects between LSPs provide a way to "stitch" together two label-switched paths, including paths that fall in two different traffic engineering database (TED) areas.

The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first interface.

For most CCC connections that connect interfaces, the interfaces must be of the same type; that is, ATM to ATM, Frame Relay to Frame Relay, PPP to PPP, or Cisco HDLC to Cisco HDLC.

ATM-to-Ethernet interworking cross-connect circuits connect logical interfaces configured on an ATM2 and Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet IQ2 and IQ2-E physical interfaces.

For all TCC connections that connect interfaces, the interfaces can be of unlike types. Mainly, TCC is used for Layer 2.5 virtual private networks (VPNs), but it can also be used as a simple “unlike circuit” switch.

Switching cross-connects join logical interfaces to form what is essentially Layer 2 switching.

**Figure 15 on page 256** illustrates a Layer 2 switching circuit cross-connect. In this topology, Router A and Router C have Frame Relay connections to Router B, which is a Juniper Networks router. CCC allows you to configure Router B to act as a Frame Relay (Layer 2) switch. To do this, configure a circuit from Router A to Router C that passes through Router B, effectively configuring Router B as a Frame Relay switch with respect to these routers. This configuration allows Router B to transparently switch packets (frames) between Router A and Router C without regard to the packets’ contents or the Layer 3 protocols. The only processing that Router B performs is to translate DLCI 600 to 750.

**Figure 15: Layer 2 Switching Circuit Cross-Connect**

---

Copyright © 2019, Juniper Networks, Inc.
If the Router A–to–Router B and Router B–to–Router C circuits are PPP, for example, the Link Control Protocol and Network Control Protocol exchanges occur between Router A and Router C. These messages are handled transparently by Router B, allowing Router A and Router C to use various PPP options (such as header or address compression and authentication) that Router B might not support. Similarly, Router A and Router C exchange keepalives, providing circuit-to-circuit connectivity status.

You can configure Layer 2 switching cross-connects on PPP, Cisco HDLC, Frame Relay, Ethernet CCC, Ethernet VLAN, and ATM circuits. With CCC, only like interfaces can be connected in a single cross-connect. With TCC, unlike interfaces can be connected in a single cross-connect. In Layer 2 switching cross-connects, the exchanges take place between point-to-point links.

This chapter discusses the Layer 2 switching cross-connect configuration tasks. For information about MPLS tunneling and LSP stitching, see the MPLS Applications Feature Guide.

For information about Layer 2 and Layer 2.5 VPNs, see the Junos OS VPNs Library for Routing Devices.

For restrictions for MPLS on QFX switches, see MPLS Feature Support on QFX Series and EX4600 Switches.

### Related Documentation
- Defining the Encapsulation for Switching Cross-Connects on page 257
- Defining the Connection for Switching Cross-Connects on page 261
- Configuring MPLS for Switching Cross-Connects on page 261
- Configuring IS-IS or MPLS Traffic for TCC Interfaces on page 262
- Configuring ATM-to-Ethernet Interworking on page 262
- Example: Configuring a CCC over Frame Relay Encapsulated Interface on page 268
- Example: Configuring a TCC on page 269
- Example: Configuring CCC over Aggregated Ethernet on page 270
- Example: Configuring a Remote LSP CCC over Aggregated Ethernet on page 272
- Example: Configuring ATM-to-Ethernet Interworking on page 274

### Defining the Encapsulation for Switching Cross-Connects
- Defining the Encapsulation for Switching Cross-Connects on page 258
- Configuring PPP or Cisco HDLC Circuits on page 258
- Configuring ATM Circuits on page 258
- Configuring Frame Relay Circuits on page 259
- Configuring Ethernet CCC Circuits on page 260
- Configuring Ethernet VLAN Circuits on page 260
Defining the Encapsulation for Switching Cross-Connects

To configure Layer 2 or Layer 2.5 switching cross-connects, configure the CCC or TCC encapsulation on the router that is acting as the switch (Router B in Figure 15 on page 256).

NOTE: When you use CCC encapsulation, you can configure the ccc family only. Likewise, when you use TCC encapsulation, you can configure the tcc family only.

This section contains the following topics:

Configuring PPP or Cisco HDLC Circuits

For PPP or Cisco HDLC circuits, specify the encapsulation by including the `encapsulation` statement at the `[edit interfaces interface-name]` hierarchy level. This statement configures the entire physical device. For these circuits to work, you must configure a logical interface unit 0.

```
[edit interfaces interface-name]
encapsulation (ppp-ccc | cisco-hdlc-ccc | ppp-tcc | cisco-hdlc-tcc);
unit 0;
```

Configuring ATM Circuits

For ATM circuits, include the `vpi` statement `[edit interfaces interface-name atm-options]` hierarchy level:

```
[edit interfaces at-fpc/pic/port]
atm-options {
    vpi vpi-identifier;
}
```

On the logical interface, include the following statements:

```
point-to-point;
encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-tcc-vc-mux | atm-tcc-snap);
vci vpi-identifier.vci-identifier;
```

You can include the logical interface statements at the following hierarchy levels:

- `[edit interfaces at-fpc/pic/port unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number]`

For each VC, configure whether it is a circuit or a regular logical interface. The default interface type is point-to-point.
Configuring Frame Relay Circuits

For Frame Relay circuits, include the encapsulation statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
encapsulation type;
```

On the logical interface, include the following statements:

```
point-to-point;
en encapsulation type;
unit dlci dlci-identifier;
```

You can include the logical interface statements at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

The encapsulation type can be one of the following:

- Flexible Frame Relay (flexible-frame-relay)—Intelligent queuing (IQ) interfaces can use flexible Frame Relay encapsulation. You use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

- Frame Relay CCC version (frame-relay-ccc)—For E1, E3, SONET/SDH, T1, and T3 interfaces, this encapsulation type is the same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC. The logical interface must also have frame-relay-ccc encapsulation. When you use this encapsulation type, you can configure the ccc family only.

- Frame Relay TCC version (frame-relay-tcc)—Similar to Frame Relay CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

- Extended CCC version (extended-frame-relay-ccc)—This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC. The logical interface must have frame-relay-ccc encapsulation. When you use this encapsulation type, you can configure the ccc family only.

- Extended TCC version (extended-frame-relay-tcc)—Similar to extended Frame Relay CCC, this encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC, which is used for circuits with different media on either side of the connection.

- Port CCC version (frame-relay-port-ccc)—Defined in the IETF document Frame Relay Encapsulation over Pseudo-Wires (expired December 2002). This encapsulation type allows you to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with
Frame Relay transport. The connection between the two CE routers can be either user-to-network interface (UNI) or network-to-network interface (NNI); this is completely transparent to the PE routers. The logical interface does not require an encapsulation statement. When you use this encapsulation type, you can configure the ccc family only.

For each DLCI, configure whether it is a circuit or a regular logical interface. The DLCI for regular interfaces must be from 1 through 511. For CCC and TCC interfaces, it must be from 512 through 1022. This restriction does not apply to IQ interfaces. The default interface type is point to point.

Configuring Ethernet CCC Circuits

You can configure Ethernet CCC encapsulation on Fast Ethernet, Gigabit Ethernet, and aggregated Ethernet interfaces.

**NOTE:** CCC over aggregated Ethernet requires an M Series Enhanced Flexible PIC Concentrator (FPC).

For Ethernet CCC circuits, specify the encapsulation by including the `encapsulation` statement at the `[edit interfaces interface-name]` hierarchy level. This statement configures the entire physical device.

```
[edit interfaces interface-name]
encapsulation ethernet-ccc;
unit logical-unit-number {
    ...
}
[edit interfaces aex]
encapsulation ethernet-ccc;
unit logical-unit-number {
    ...
}
```

Configuring Ethernet VLAN Circuits

You can configure Ethernet virtual local area network (VLAN) circuits on Fast Ethernet, Gigabit Ethernet, and aggregated Ethernet interfaces. For Ethernet VLAN circuits, specify the encapsulation by including the `encapsulation` statement at the `[edit interfaces interface-name]` hierarchy level. This statement configures the entire physical device. You must also enable VLAN tagging. To do this, include the following statements:

```
[edit interfaces interface-name]
vlan-tagging;
encapsulation (extended-vlan-ccc | vlan-ccc);
[edit interfaces aex]
vlan-tagging;
encapsulation vlan-ccc;
```

On the logical interface, include the following statements:
encapsulation vlan-ccc;
  vlan-id number;

You can include the logical interface statements at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Ethernet interfaces in VLAN mode can have multiple logical interfaces. For encapsulation type `vlan-ccc`, VLAN IDs 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 1023 are reserved for CCC VLANs. For encapsulation type `extended-vlan-ccc`, VLAN IDs 1 through 4094 are valid. VLAN ID 0 is reserved for tagging the priority of frames.

See Also
- Figure 15 on page 256
- Circuit and Translational Cross-Connects Overview on page 255

**Defining the Connection for Switching Cross-Connects**

To configure Layer 2 switching cross-connects, define the connection between the two circuits. You configure this on the router that is acting as the switch (Router B in Figure 15 on page 256). The connection joins the interface that comes from the circuit’s source to the interface that leads to the circuit’s destination. When you specify the interface names, include the logical portion of the name, which corresponds to the logical unit number. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first interface.

```
[edit protocols]
connections {
  remote-interface-switch connection-name {
    interface interface-name.unit-number;
  }
  lsp-switch connection-name {
    transmit-lsp lsp-number;
    receive-lsp lsp-number;
  }
}
```

**Configuring MPLS for Switching Cross-Connects**

For Layer 2 switching cross-connects to work, you must configure MPLS. The following is a minimal MPLS configuration:

```
[edit protocols]
mpls {
  interface (interface-name | all);
}
```
Configuring IS-IS or MPLS Traffic for TCC Interfaces

Layer 2.5 VPNs on T Series, M120, MX Series, and M320 routers support IPv4, IS-IS, and MPLS traffic types. By default, IPv4 traffic runs on T Series, M120, MX Series, and M320 routers and over TCC interfaces. To configure IS-IS (ISO traffic) or MPLS traffic on Layer 2.5 VPNs, you must configure the same traffic type on both ends of the Layer 2.5 VPN.

**NOTE:** Some platform and FPC combinations cannot pass TCC encapsulated ISO traffic. See Platforms/FPCs That Cannot Forward TCC Encapsulated ISO Traffic for details.

To specify which traffic can run over a TCC interface, include the protocols statement with the appropriate value (inet, mpls, and iso) at the [edit interfaces interface-name unit logical-unit-number family tcc] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family tcc]
protocols [inet iso mpls ];
```

**NOTE:** Layer 2.5 VPNs running on M Series Multiservice Edge Routers support only IPv4 traffic. IPv6 is not supported on Layer 2.5 VPNs.

When enabling ISO over a Layer 2.5 VPN that is configured on a CE Ethernet interface, you must also include the point-to-point statement at the [edit protocols isis interface interface-name] hierarchy level:

```
[edit protocols isis interface interface-name]
point-to-point;
```

For more information about Layer 2.5 VPNs, see the Junos OS VPNs Library for Routing Devices and the Translational Cross-Connect and Layer 2.5 VPNs Feature Guide.

Configuring ATM-to-Ethernet Interworking

- ATM-to-Ethernet Interworking on page 263
- Enabling ATM-to-Ethernet Interworking on page 263
- Configuring the Ethernet Interface on page 264
- Configuring Ethernet Encapsulation on page 264
- Configuring the Outer VLAN Identifier on page 264
- Configuring the Inner VLAN Identifier Range on page 264
ATM-to-Ethernet Interworking

The ATM-to-Ethernet interworking feature is useful where ATM2 interfaces are used to terminate ATM DSLAM traffic. The ATM traffic can be forwarded with encapsulation type ccc (circuit cross-connect) to a local or remote Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet IQ2 and IQ2-E interface or label-switched path (LSP). The ATM VPI and VCI are converted to stacked VLAN inner and outer VLAN tags.

These ATM-to-Ethernet interworking circuits can be mapped to individual logical interfaces configured on an ATM2 IQ interface and Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet IQ2 and IQ2-E physical interface.

The ATM-to-Ethernet interworking cross-connect essentially provides Layer 2 switching, and statistics are reported at the logical interface level.

During conversion from ATM to Ethernet, the least significant 12 bits of the ATM cell VCI are copied to the Ethernet frame inner VLAN tag. Cells received on an ATM logical interface configured with encapsulation type vlan-vci-ccc and falling within the configured VCI range are reassembled into packets and forwarded to a designated Ethernet logical interface that is configured with encapsulation type vlan-vci-ccc.

During conversion from Ethernet to ATM, the Ethernet frame inner VLAN tags that fall within the configured range, are copied to the least significant 12 bits of the ATM cell VCI. The ATM logical interface uses its configured VPI when segmenting the Ethernet packets into cells.

ATM-to-Ethernet interworking is supported on M120, M320, and T Series routers.

ATM-to-Ethernet interworking is supported on MX Series routers with aggregated Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces. This feature is available on all Enhanced Queuing (EQ) DPCs and Enhanced DPCS for MX Series routers.

NOTE: This feature is not supported on MX Series routers with ATM interfaces.

For more information on MX Series ATM-to-Ethernet interworking, see the MX Series Solutions Guide.

The following sections discuss ATM-to-Ethernet interworking:

Enabling ATM-to-Ethernet Interworking

To enable the ATM-to-Ethernet interworking cross-connect function, include the vlan-vci-tagging statement at the [edit interfaces interface-name] hierarchy level:
[edit interfaces interface-name]
  vlan-vci-tagging;

Configuring the Ethernet Interface

Configure the Ethernet or aggregated Ethernet physical interface by including the `encapsulation` statement with the `vlan-vci-ccc` option at the `[edit interfaces interface-name]` hierarchy level:

[edit interfaces interface-name]
  encapsulation vlan-vci-ccc;

When the encapsulation type `vlan-vci-ccc` is configured on the physical interface, all logical interfaces configured on the Ethernet interface must also have the encapsulation type set to `vlan-vci-ccc`.

Configuring Ethernet Encapsulation

Configure the Ethernet logical interface by including the `encapsulation` statement with the `vlan-vci-ccc` option at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

[edit interfaces interface-name unit logical-unit-number]
  encapsulation vlan-vci-ccc;

The chassis configuration cannot contain the `atm-l2circuit-mode` statement if any logical interfaces are configured with the `vlan-vci-ccc` encapsulation option.

Configuring the Outer VLAN Identifier

Configure the Ethernet logical interface outer VLAN ID by including the `vlan-id` statement specifying the outer VLAN ID at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

[edit interfaces interface-name unit logical-unit-number]
  vlan-id outer-vlan-identifier;

It is the administrator’s responsibility to ensure that the outer VLAN tag and VPI match and the inner VLAN tags fall within the VCI range of the VPI.

The allowable VPI range is from 0 to 255. So the outer VLAN tags must not be configured for values above 255.

Configuring the Inner VLAN Identifier Range

Configure the Ethernet logical interface inner VLAN ID range by including the `inner-vlan-id-range` statement and specifying the starting VLAN ID and ending VLAN ID at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

[edit interfaces interface-name unit logical-unit-number]
  inner-vlan-id-range start start-id end end-id;
VLAN IDs 0 and 4095 are reserved by IEEE 801.1q and must not be used for the inner or outer VLAN ID.

VCIs 0 through 31 are reserved for ATM management purposes by convention. Therefore inner VLAN IDs 1 through 31 should not be used.

VLAN ID 1 might be used by Ethernet switches for certain bridge management services, so using VLAN ID 1 for the inner or outer VLAN ID is discouraged.

**Configuring the Physical Interface VPI**

Configure the ATM physical interface VPI by including the `vpi` statement at the `[edit interfaces interface-name atm-options]` hierarchy level:

```
[edit interfaces interface-name atm-options]
vpi virtual-path-identifier;
```

VPI 0 is reserved, and must not be used.

ATM F4/F5 OAM is not supported for VPIs used in ATM-to-Ethernet interworking cross-connects. Any F4/F5 OAM cells received are discarded.

Only one logical interface may be declared per virtual path specified in the `atm-options` statement hierarchy.

It is not necessary to dedicate all the VPIs of an ATM2 interface for ATM-to-Ethernet interworking cross-connects.

**Configuring the ATM Logical Interface**

Configure the ATM logical interface by including the `encapsulation` statement and specifying the encapsulation type `vlan-vci-ccc` at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
encapsulation vlan-vci-ccc;
```

An ATM logical interface configured with the encapsulation type `vlan-vci-ccc` only supports the `epd-threshold`, `shaping`, `traps | no-traps`, `disable`, and `description` statements. No other configuration statements are supported. ATM interface CoS features are not supported by logical interfaces configured with the encapsulation type `vlan-vci-ccc`.

The ATM2 OC48 PIC does not support the encapsulation type `vlan-vci-ccc`.

The encapsulation type `vlan-vci-ccc` only supports the `ccc` protocol family. Attempts to configure any other interface protocol family are rejected.

**Configuring the Protocol Family**

Configure the ATM logical interface protocol family by including the `family` statement and specifying the `ccc` option at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:
[edit interfaces interface-name unit logical-unit-number]
family ccc;

Configuring the Logical Interface VPI

Configure the ATM logical interface virtual path identifier by including the `vpi` statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
  vpi virtual-path-identifier;
```

VPI 0 is reserved, and must not be used.

It is the administrator’s responsibility to ensure the outer VLAN tag and VPI match and the inner VLAN tags fall within the VCI range of the VPI.

Once a VPI is used in an ATM-to-Ethernet interworking cross-connect, it cannot be used with any other logical interface, even if the `vpi.vci` value falls outside the VCI range for the cross-connect.

Configuring the Logical Interface VCI

Configure the ATM logical interface virtual channel identifier range by including the `vci-range` statement and specifying the starting VCI and ending VCI at the [edit interfaces interface-name unit logical-unit-number] hierarchy level:

```plaintext
[edit interfaces interface-name unit logical-unit-number]
  vci-range start start-vci end end-vci;
```

Do not use VCIs 0 through 31, which are reserved for ATM management purposes by convention.

See Also
- encapsulation on page 567
- family on page 603
- inner-vlan-id-range on page 678
- vci-range on page 1116
- vlan-id on page 1118
- vlan-vci-tagging on page 1137
- vpi (ATM CCC Cell-Relay Promiscuous Mode) on page 1137
- vpi (Logical Interface and Interworking) on page 1139
ATM-To-Ethernet Interworking on ATM MICs

ATM-to-Ethernet interworking supports transmission of ATM packets over Ethernet. It specifically provides support for exchange of Layer 2 and Layer 3 Protocol Data Units (PDUs) between ATM and Ethernet domains. On MX Series 5G Universal Routing Platforms with ATM MICs, you can exchange Ethernet frames between ATM and Ethernet domains over a MPLS pseudowire or a Layer 2 cross-connect by using translational cross connect (TCC). For more information about TCC, see “Circuit and Translational Cross-Connects Overview” on page 255.

Consider the following basic ATM-to-Ethernet Interworking topology where the provider edge router PE1 is connected to an ATM domain and the Provider Edge router PE2 is connected to an Ethernet domain (see Figure 1). The customer edge routers CE1 and CE2 are customer-managed devices. The PE routers are connected by means of an MPLS pseudowire. The ATM traffic on the PE1–CE1 link can comprise untagged Ethernet frames over ATM format. The Ethernet traffic on PE2–CE2 link can comprise untagged, single-VLAN or double-VLAN tagged Ethernet frames depending on the configuration of the PE2 router.

For ATM-to-Ethernet Interworking, the virtual path identifier (VPI) and virtual circuit identifier (VCI) values on the ATM link are mapped to the outer and inner VLAN tag on the Ethernet link. Mapping implies that either the same value is copied or a one-to-one translation is performed. If VLAN translation is enabled, instead of copying the value, a one-to-one translation is performed on the Ethernet facing PE, using a lookup table.

ATM cells that are received on the PE1 router are reassembled into ATM Adaptation Layer 5 (AAL5) logical link control (LLC) frames. The router removes the header and footer and adds two VLAN tags (outer and inner) to the untagged Ethernet payload based on the configuration. The VLAN IDs must correspond to the VPI and VCI of the ATM cell. You must add an MPLS label before transmitting the dual-VLAN-tagged Ethernet frame over the MPLS pseudowire. You can also add other optional MPLS tags.

NOTE: If the AAL5 frame sent by CE1 is not encapsulated with LLC and if the untagged Ethernet payload includes the frame check sequence (FCS), PE1 rejects the AAL5 frame. Also, PE1 can transmit and receive only a dual VLAN-tagged Ethernet frame without FCS. Inclusion of FCS can result in packet drops or data corruption.

On the PE2 router, the MPLS label and optional MPLS tags are removed and the Ethernet frame is transmitted toward the CE2 router. You can modify or remove one or both VLAN tags before forwarding the frame to the CE2 router.

Limitations

Following are the limitations of the ATM-to-Ethernet interworking feature on MX Series routers with ATM MICs:
• The ATM-to-Ethernet interworking feature is not backward compatible or does not interoperate with the ATM-Ethernet interworking feature supported on M Series and T Series Routers. The functionality is the same but the implementation is different.

• The total number of VCIs supported is 4000 for the ATM MIC. This is an existing system limit.

• If an ATM logical interface is configured with vci-range of N VCIs, then N VCIs are deducted from the available pool of 4000 VCIs.

• ATM quality of service (QoS) is not supported with the vlan-vci-ccc encapsulation. If you use the vci-range statement then the vlan-vci-ccc encapsulation supports multiple VCIs on a single logical interface. This is a hardware limitation.

Related Documentation

Example: Configuring ATM-to-Ethernet Interworking on ATM MIC on page 275

Example: Configuring a CCC over Frame Relay Encapsulated Interface

Configure a full-duplex Layer 2 switching circuit cross-connect between Router A and Router C, using a Juniper Networks router, Router B, as the virtual switch. See the topology in Figure 16 on page 268.

Figure 16: Example Topology of a Switching Circuit Cross-Connect with Frame Relay CCC Encapsulation

```conf
[edit]
interfaces {
  so-1/0/0 {
    encapsulation frame-relay-ccc;
    unit 1 {
      point-to-point;
      eui-64 frame-relay-ccc;
      dlci 600;
    }
  }
  so-2/0/0 {
    encapsulation frame-relay-ccc;
    unit 2 {
      point-to-point;
      encapsulation frame-relay-ccc;
      dlci 750;
    }
  }
}
protocols {
  connections {
```

268 Copyright © 2019, Juniper Networks, Inc.
interface-switch router-a-router-c {
    interface so-1/0/0.1;
    interface so-2/0/0.2;
}
}

mpls {
    interface all;
}
}

Related Documentation

• Configuring Layer 2 Switching Cross-Connects Using CCC

Example: Configuring a TCC

Configure a full-duplex switching translational cross-connect with PPP TCC encapsulation between Router A and Router C, using a Juniper Networks router, Router B, as the virtual switch. See the topology in Figure 17 on page 269.

In this topology, Router B has a PPP connection to Router A and an ATM connection to Router C.

Figure 17: Layer 2.5 Switching Translational Cross-Connect

On Router A

```
[edit]
interfaces {
    so-0/1/0 {
        description "to Router B so-1/0/0";
        encapsulation ppp;
        unit 0 {
            family inet {
                address 10.1.1.30;
            }
        }
    }
}
```

On Router B

```
[edit]
interfaces {
    so-1/0/0 {
        description "to Router A so-0/1/0";
        encapsulation ppp-tcc;
        unit 0 {
        }
    }
    at-1/1/0 {
```
On Router C

description "to Router C at-0/3/0";
atm-options {
   vpi 0 maximum-vcs 2000;
}
unit 32 {
   vci 32;
   encapsulation atm-tcc-vc-mux;

}

Related Documentation

Example: Configuring CCC over Aggregated Ethernet

See the topology in Figure 18 on page 271. In this topology, CE Routers A and C have aggregated Ethernet connections to PE Router B. With CCC, you specify that the circuit from Router A is connected to the circuit from Router C. Router B functions as a cross-connect switch between the two circuits. For a back-to-back connection, all VLAN IDs must be the same on Router A through Router C. You configure Router A and Router
C as standard aggregated Ethernet interfaces. For more information about aggregated Ethernet, see "Aggregated Ethernet Interfaces Overview."

Figure 18: Interface-to-Interface Circuit Cross-Connect over Aggregated Ethernet Interfaces

On Router A
[edit interfaces]
ae0 {
    vlan-tagging;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 1g;
    }
    unit 0 {
        vlan-id 600;
        family inet {
            address 192.168.1.1/30;
        }
    }
}

On Router B
[edit interfaces]
ae0 {
    encapsulation vlan-ccc;
    vlan-tagging;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 1g;
    }
    unit 0 { # CCC switch
        encapsulation vlan-ccc;
        vlan-id 600;
        family ccc;
    }
ae1 {
    encapsulation vlan-ccc;
    vlan-tagging;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 100m;
    }
    unit 0 {
        encapsulation vlan-ccc;
        vlan-id 600;
        family ccc;
    }
}
[edit protocols]
mpls {
    interface all;
}
connections {
    interface-switch layer2-cross-connect {
        interface ae0.0;
        interface ae1.0;
    }
}

On Router C
[edit interfaces]
ae1 {
    vlan-tagging;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 1g;
    }
    unit 0 {
        vlan-id 600;
        family inet {
            address 192.168.12/30;
        }
    }
}

Example: Configuring a Remote LSP CCC over Aggregated Ethernet

See the topology in Figure 19 on page 272. In this topology, CE Router G has an aggregated Ethernet connection to PE Router F. CE Router D has an aggregated Ethernet connection to PE Router E. Router E and Router F have an MPLS LSP between them. With remote CCC, you specify that the circuit from Router D is connected to the circuit from Router G. The circuit from Router D is connected to the LSP on Router E; the circuit from Router G is connected to the LSP on Router F. In other words, ae0.0 and ae1.0 are connected using lsp1-2 and lsp2-1. You configure Router D and Router G as standard aggregated Ethernet interfaces. For more information about aggregated Ethernet, see Aggregated Ethernet Interfaces Overview.

Figure 19: Remote Interface-LSP-Interface Circuit Cross-Connect over Aggregated Ethernet Interfaces

On Router D
[edit interface]
ae0 {
    aggregated-ether-options {
        minimum-links 1;
        link-speed 1g;
    }
}
lacp {
    active;
    periodic fast;
}
}
unit 0 {
    family inet {
        address 192.168.2.1/30;
    }
}
}

On Router E
  [edit interfaces]
  ae0 {
    encapsulation ethernet-ccc;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 100m;
        lacp {
            active;
            periodic fast;
        }
    }
    unit 0 {
        encapsulation vlan-ccc; # default
        family ccc; # default
    }
  }
  [edit protocols]
  mpls {
    interface all;
  }
  connections {
    remote-interface-switch remote-sw-1 {
        interface ae0.0;
        receive-lsp lsp2_1;
        transmit-lsp lsp1_2;
    }
  }

On Router F
  [edit interfaces]
  ae1 {
    encapsulation ethernet-ccc;
    aggregated-ether-options {
        minimum-links 1;
        link-speed 100m;
        lacp {
            active;
            periodic fast;
        }
    }
    unit 0 {

encapsulation vlan-ccc; # default
family ccc; # default

}]
[edit protocols]
mpls {
  interface all;
}
connections {
  remote-interface-switch remote-sw-2 {
    interface ae1.0;
    receive-lsp lsp1_2;
    transmit-lsp lsp2_1;
  }
}

On Router G
[edit interface]
ae1 {
  aggregated-ether-options {
    minimum-links 1;
    link-speed 1g;
    lacp {
      active;
      periodic fast;
    }
  }
  unit 0 {
    family inet {
      address 192.168.2.2/30;
    }
  }
}

Example: Configuring ATM-to-Ethernet Interworking

The following example shows the configuration of the ATM and Ethernet interfaces for an ATM-to-Ethernet interworking cross connect. In the example ATM DSLAM traffic is terminated on an ATM2 interface. The ATM traffic is forwarded using encapsulation type `vlan-vci-ccc` to a local Ethernet IQ2 and IQ2-E interface. See the topology in Figure 20 on page 274.

Figure 20: ATM-to-Ethernet Interworking

In this example, the ATM traffic comes from the DSLAM to the router on ATM interface `at-4/0/0` and is forwarded out on Ethernet interface `ge-2/2/1`.
[edit interfaces]
ge-2/2/1 {
  vlan-vci-tagging;
  encapsulation vlan-vci-ccc;
  unit 0 {
    encapsulation vlan-vci-ccc;
    vlan-id 100;
    inner-vlan-id-range start 100 end 500;
  }
}
at-4/0/0 {
  atm-options {
    vpi 100;
  }
  unit 0 {
    encapsulation vlan-vci-ccc;
    family ccc;
    vpi 100;
    vci-range start 100 end 500;
  }
}

Related Documentation

• Configuring ATM-to-Ethernet Interworking on page 262

Example: Configuring ATM-to-Ethernet Interworking on ATM MIC

This example shows how to configure the ATM and Ethernet interfaces for an ATM-to-Ethernet interworking cross-connect.

• Requirements on page 275
• Overview on page 275
• Configuration on page 276

Requirements

This example uses the following hardware and software components:

• One MX Series router with ATM MIC
• One MX Series router with Ethernet MIC
• Junos OS Release 16.1R1 or later release

Overview

Configuring ATM-to-Ethernet interworking enables exchange of Ethernet frames between an ATM domain and an Ethernet domain on MX Series routers with ATM MIC. The ATM domain can be connected to the Ethernet domain over an MPLS pseudowire.
Topology

Consider a sample topology in which provider edge (PE) router (ATMRouter) is an MX Series router with an ATM MIC and PE router (EthernetRouter) is an MX Series router with an Ethernet MIC. CE1 and CE2 are the customer edge routers or customer-managed devices. ATMRouter and EthernetRouter are connected by means of an MPLS pseudowire. The ATM traffic between ATMRouter and CE1 comprises untagged Ethernet over ATM cells. The Ethernet traffic between EthernetRouter and CE2 comprises double-VLAN-tagged Ethernet frames.

When a packet is sent from CE1 to CE2 (ATM-to-Ethernet), ATMRouter accepts ATM cells from CE1 with virtual circuit identifier (VCI) in the range 10/50 to 10/100 and reassembles ATM cells into AAL5 frames. ATMRouter extracts the Ethernet frame from the AAL5 frame payload. ATMRouter adds two VLAN tags with VLAN IDs corresponding to the virtual path identifier (VPI) and VCI of the received ATM cell. The dual-tagged-Ethernet frame is then encapsulated into a MPLS packet and sent over the pseudowire to EthernetRouter.

EthernetRouter strips the MPLS encapsulation and the dual-VLAN-tagged Ethernet frame is sent to CE2. The outer VLAN ID is rewritten to 20 and the inner VLAN ID remains the same. The packet arrives at CE2.

The reverse happens when a packet is sent from CE2 to CE1.

Configuration

To enable exchange of Ethernet frames between an ATM domain and an Ethernet domain according to the topology mentioned in the overview section, perform these tasks:

- Configuring ATMRouter on page 276
- Configuring EthernetRouter on page 279

Configuring ATMRouter

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 in the CLI User Guide.

To configure the interfaces on ATMRouter:

1. To configure the MIC to use SONET framing, include the framing statement at the [edit chassis] hierarchy level.

   [edit chassis]
   user@host# set fpc 1 pic 0 framing sonet port 0 framing sonet speed oc3-stm1

2. In configuration mode, go to the [edit interfaces] hierarchy level. Configure the Ethernet core interface that connects ATMRouter to EthernetRouter and specify the description of the Ethernet interface for your reference.
3. Configure a logical unit for the Ethernet interface, specify the family as `/inet`, and assign an IP address to the interface. Also, specify the family as `/mpls` to enable ATMRouter to connect to EthernetRouter.

    [edit interfaces ge-1/0/0]
    user@host# edit unit 0
    user@host# set family inet address 192.0.0.1/24
    user@host# set family mpls
    user@host# top

4. In configuration mode, at the [edit interfaces] hierarchy level, configure the ATM interface that connects to CE1 and specify the description of the ATM interface for your reference. Also, define the virtual path identifier for this interface by using the `vpi` statement and specify a value from 1 through 255. The value zero (0) is reserved and must not be used.

    [edit]
    user@host# edit interfaces
    user@host# edit at-1/2/0
    user@host# set description CE1Facing
    user@host# set atm-options vpi 10

5. Configure a logical unit for the ATM interface. Also, configure the ATM logical interface by specifying the encapsulation and the protocol family. The encapsulation type `vlan-vci-vcc` supports only the `ccc` protocol family. Any attempts to configure any other interface protocol family is rejected.

    [edit interfaces at-1/2/0]
    user@host# edit unit 0
    user@host# set encapsulation vlan-vci-vcc family ccc

6. Configure the VPI and VCI for the logical interface. The VPI value 0 is reserved and must not be used. VCI values from 0 through 31 are reserved for ATM management purposes by convention.

    [edit interfaces at-1/2/0 unit 0]
    user@host# set vpi 10 vci-range start 100 end 110
    user@host# top

7. Configure the physical loopback interface at the [edit interfaces] hierarchy level.

    [edit]
8. Configure the route identifier that specifies the routing device's IP address. The router identifier is used by BGP and OSPF to identify the routing device from which a packet originated. The router identifier is usually the IP address of the local routing device. If you do not configure a router identifier, the IP address of the first interface to come online is used. This is usually the loopback interface. Otherwise, the first hardware interface with an IP address is used.

   [edit]
   user@host# set router-options router-id 198.51.100.1

9. At the [edit protocols] hierarchy level, configure the interface on which to configure MPLS as well as the loopback interface.

   [edit protocols]
   user@host# edit mpls
   user@host# set interface ge-1/0/0.0
   user@host# set interface lo0.0
   user@host# top

10. At the [edit protocols] hierarchy level, configure a single-area OSPF network by specifying the area ID and associated interfaces (Ethernet interface and the loopback interface).

    [edit protocols]
    user@host# edit ospf
    user@host# set area 0.0.0.0 interface ge-1/0/0.0
    user@host# set area 0.0.0.0 interface lo0.0
    user@host# top

11. Create an LDP instance on the Ethernet interface and the loopback interface at the [edit] hierarchy level. LDP is required as the signaling protocol for Layer 2 circuits.

    [edit]
    user@host# edit protocols ldp
    user@host# set interface ge-1/0/0.0
    user@host# set interface lo0.0
    user@host# top

12. Establish the Layer 2 circuit by specifying the l2circuit statement at the [edit protocols] hierarchy level. The neighbor parameter specifies the IP address of the PE neighbor. The interface name refers to the local CE-facing interface that forms the Layer 2 circuit. The VCI ID must match the ID of the PE neighbor.

    [edit]
    user@host# edit protocols l2circuit
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 in the CLI User Guide.

To configure the interfaces on EthernetRouter:

1. In configuration mode, go to the [edit interfaces] hierarchy level. Configure the Ethernet core interface that connects EthernetRouter to ATMRouter and specify the description of the Ethernet interface for your reference.

   ```
   [edit]
   user@host# edit interfaces
   user@host# edit ge-1/0/0
   user@host# set description PE1Facing
   ```

2. Configure a logical unit for the Ethernet interface and specify the family as inet and assign an IP address to the Ethernet interface. Also, specify the family as mpls to enable EthernetRouter to connect to ATMRouter.

   ```
   [edit interfaces ge-1/0/0]
   user@host# edit unit 0
   user@host# set family inet address 192.0.0.2/24
   user@host# set family mpls
   user@host# top
   ```

3. At the [edit interfaces] hierarchy level, configure the Ethernet interface that connects to CE2 and specify the description of the interface for your reference. Also, specify flexible-vlan-tagging to support transmission of 802.1Q VLAN single-tag and dual-tag frames on the same port. Specify extended-vlan-ccc as the encapsulation to enable tagging for translational cross-connect (TCC).

   ```
   [edit]
   user@host# edit interfaces
   user@host# edit ge-1/0/1
   user@host# set description CE2Facing
   user@host# set flexible-vlan-tagging
   user@host# set encapsulation extended-vlan-ccc
   user@host# set gigether-options ethernet-switch-profile tag-protocol-id [0x8100 0x9100 0x88a8]
   ```
4. Configure a logical unit for the Ethernet interface. Also, configure mixed tagging. Mixed tagging enables you to configure two logical interfaces on the same Ethernet port, one with single-tag framing and one with dual-tag framing. You can also specify the protocol family.

```
[edit interfaces ge-1/0/1]
user@host# edit unit 0
user@host# set vlan-tags outer 0x88a8.10 inner-range 0x8100.100-110
user2host# set family ccc;
```

5. Configure the physical loopback interface at the [edit interfaces] hierarchy level.

```
[edit]
user@host# set interfaces lo0 unit 0 family inet address 198.51.100.2/32
```

6. Configure the route identifier that specifies the routing device's IP address. The router identifier is used by BGP and OSPF to identify the routing device from which a packet originated. The router identifier is usually the IP address of the local routing device. If you do not configure a router identifier, the IP address of the first interface to come online is used. This is usually the loopback interface. Otherwise, the first hardware interface with an IP address is used.

```
[edit]
user@host # set router-options router-id 198.51.100.2
```

7. At the [edit protocols] hierarchy level, configure the interface on which to configure MPLS as well as the loopback interface.

```
[edit protocols]
user@host# edit mpls
user@host# set interface ge-1/0/0.0
user@host# set interface lo0.0
user@host# top
```

8. At the [edit protocols] hierarchy level, configure a single-area OSPF network by specifying the area ID and associated interfaces (Ethernet interface and the loopback interface).

```
[edit protocols]
user@host# edit ospf
user@host# set area 0.0.0.0 interface ge-1/0/0.0
user@host# set area 0.0.0.0 interface lo0.0
user@host# top
```

9. Create an LDP instance on the Ethernet interface and the loopback interface at the [edit] hierarchy level. LDP is required as the signaling protocol for Layer 2 circuits.

```
[edit]
```
user@host# edit protocols ldp
user@host# set interface ge-1/0/0.0
user@host# set interface lo0.0
user@host# top

10. Establish the Layer 2 circuit by specifying the l2circuit statement at the [edit protocols] hierarchy level. The neighbor parameter specifies the IP address of the PE neighbor. The interface name refers to the local CE-facing interface that forms the Layer 2 circuit. The VCI ID must match the ID of the PE neighbor.

[edit]
user@host# edit protocols l2circuit
user@host# edit neighbor 198.51.100.1 interface ge-1/0/1.0
user@host# set static incoming label 1000000 outgoing label 1000000
user@host# set virtual-circuit-id 5
user@host# set no-control-word
user@host# set ignore-encapsulation-mismatch
user@host# set ignore-mtu-mismatch

Related Documentation
• ATM-To-Ethernet Interworking on ATM MICs on page 267
• Verifying ATM-to-Ethernet Interworking Configuration on ATM MICs on page 281

Verifying ATM-to-Ethernet Interworking Configuration on ATM MICs

To verify that the ATM-to-Ethernet interworking feature is configured correctly, perform these tasks on both the routers:

• Verifying That The ATM Interface on Router1 Is Configured Correctly on page 281
• Verifying The Status of the MIC on Router1 on page 282
• Verify That OSPF Configuration on Router1 Is Accurate on page 282
• Verify That LDP Configuration on Router1 Is Accurate on page 283
• Verify That Layer 2 Virtual Circuit Session Configuration on Router1 Is Accurate on page 283
• Verifying That the Ethernet Interface on Router2 Is Configured Correctly on page 284
• Verifying the Status of the MIC on Router2 on page 284
• Verify That OSPF Configuration on Router2 Is Accurate on page 284
• Verify That LDP Configuration on Router2 Is Accurate on page 285
• Verify That Layer 2 Virtual Circuit Session Configuration on Router2 Is Accurate on page 285

Verifying That The ATM Interface on Router1 Is Configured Correctly

Purpose To verify that the ATM interface (at-1/2/0) on Router1 is configured correctly.
Action  From operational mode, enter the `show interfaces` command.

```
user@host> show interfaces at-1/2/0 terse
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-1/2/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>at-1/2/0.0</td>
<td>up</td>
<td>up</td>
<td>ccc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>at-1/2/0.32767</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Meaning  The ATM interface on Router1 is operational.

**Verifying The Status of the MIC on Router1**

**Purpose**  To verify the status of the MIC.

Action  From operational mode, enter the `show chassis fpc pic-status` command.

```
user@host> show chassis fpc pic-status
```

```
Slot 0 Online
PIC 2 Online 10x 1GE(LAN) -EH SFP
PIC 3 Online 10x 1GE(LAN) -EH SFP
Slot 1 Online
PIC 0 Online 2xOC12/8xOC3 CC-CE
PIC 2 Online 10x 1GE(LAN) SFP
PIC 3 Online 10x 1GE(LAN) SFP
Slot 2 Online
PIC 0 Online 4x 10GE(LAN) SFP+
```

Meaning  ATM MIC on FPC slot 1 is online and operational.

**Verify That OSPF Configuration on Router1 Is Accurate**

**Purpose**  To verify that routers are adjacent and able to exchange OSPF data.

Action  From operational mode, enter the `show ospf neighbor` command.

```
user@host> show ospf neighbor
```

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.1</td>
<td>ge-1/0/0.0</td>
<td>Full</td>
<td>198.51.100.2</td>
<td>128</td>
<td>36</td>
</tr>
</tbody>
</table>

Meaning  The adjacent router is online and can accept OSPF data.
Verify That LDP Configuration on Router1 Is Accurate

**Purpose**
To view LDP session information.

**Action**
From operational mode, enter the `show ldp session` command.

```
user@host> show ldp session
Address State Connection Hold time Adv. Mode
198.51.100.2 Operational Open 26 DU
```

**Meaning**
The output indicates that the session is operational and that the connection is open. It also indicates that the session will close in 26 seconds.

---

Verify That Layer 2 Virtual Circuit Session Configuration on Router1 Is Accurate

**Purpose**
To view the Layer 2 virtual circuits from the local PE router (Router1) to its neighbors.

**Action**
From operational mode, enter the `show l2circuit connections` command.

```
user@host> show l2circuit connections
Layer-2 Circuit Connections:
Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- Hot-standby Connection
XX -- unknown
Legend for interface status
Up -- operational
Dn -- down

Neighbor: 198.51.100.2
  Interface Type St Time last up # Up trans
  at-1/0/0.0(vc 5) rmt Up May 24 22:01:44 2016
1
  Remote PE: 198.51.100.2, Negotiated control-word: No Encapsulation: VLAN
  Incoming label: 299776, Outgoing label: 300192
  Negotiated PW status TLV: No
  Local interface: at-1/0/0.0, Status: Up, Encapsulation: VLAN Qin-Q
  and VCI Interworking
  Flow Label Transmit: No, Flow Label Receive: No
```
Verifying That the Ethernet Interface on Router2 Is Configured Correctly

**Purpose**
To verify that the Ethernet interface (ge-1/0/1) on Router2 is configured correctly.

**Action**
From operational mode, enter the `show interfaces` command.

```
user@host> show interfaces ge-1/0/1 terse
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/1</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td>ccc</td>
</tr>
<tr>
<td>ge-1/0/1.0</td>
<td>up</td>
<td>up</td>
<td>ccc</td>
<td>up</td>
<td>multiservice</td>
</tr>
<tr>
<td>ge-1/0/1.32767</td>
<td>up</td>
<td>up</td>
<td>multiservice</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**
The Ethernet interface on Router2 is operational.

Verifying the Status of the MIC on Router2

**Purpose**
To verify the status of the MIC.

**Action**
From operational mode, enter the `show chassis fpc pic-status` command.

```
user@host> show chassis fpc pic-status
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Online</th>
<th>MPC Type</th>
<th>3D</th>
<th>Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Online</td>
<td>1 3D Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC 0</td>
<td>Online</td>
<td>10x 1GE(LAN) SFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC 1</td>
<td>Online</td>
<td>10x 1GE(LAN) SFP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC 2</td>
<td>Online</td>
<td>2xOC12/8xOC3 CC-CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC 0</td>
<td>Online</td>
<td>4x 10GE(LAN) SFP+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**
MIC 2 on MPC slot 2 is online and operational.

Verify That OSPF Configuration on Router2 Is Accurate

**Purpose**
To verify that routers are adjacent and able to exchange OSPF data.

**Action**
From operational mode, enter the `show ospf neighbor` command.

```
user@host> show ospf neighbor
```

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.1</td>
<td>ge-1/0/0.0</td>
<td>Full</td>
<td>198.51.100.0</td>
<td>128</td>
<td>32</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
### Verify That LDP Configuration on Router2 Is Accurate

**Purpose**
To view LDP session information.

**Action**
From operational mode, enter the `show ldp session` command.

```bash
user@host> show ldp session
Address State       Connection Hold time Adv. Mode
198.51.100.0   Operational Open    22 DU
```

**Meaning**
The output indicates that the session is operational and that the connection is open. It also indicates that the session will close in 22 seconds.

### Verify That Layer 2 Virtual Circuit Session Configuration on Router2 Is Accurate

**Purpose**
To view the Layer 2 virtual circuits from the local PE router (Router2) to its neighbors.

**Action**
From operational mode, enter the `show l2circuit connections` command.

```bash
user@host> show l2circuit connections
Layer-2 Circuit Connections:
Legend for connection status (St)
EI -- encapsulation invalid NP -- interface h/w not present
MM -- mtu mismatch Dn -- down
EM -- encapsulation mismatch VC-Dn -- Virtual circuit Down
CM -- control-word mismatch Up -- operational
VM -- vlan id mismatch CF -- Call admission control failure
OL -- no outgoing label IB -- TDM incompatible bitrate
NC -- intf encap not CCC/TCC TM -- TDM misconfiguration
BK -- Backup Connection ST -- Standby Connection
CB -- rcvd cell-bundle size bad SP -- Static Pseudowire
LD -- local site signaled down RS -- remote site standby
RD -- remote site signaled down HS -- Hot-standby Connection
XX -- unknown
Legend for interface status
Up -- operational
Dn -- down

Neighbor: 198.51.100.0
Interface Type St Time last up # Up
trans 198.51.100.0 ge-1/0/1.0(vc 5) rmt Up May 24 22:01:45 2016 1
Remote PE: 198.51.100.0, Negotiated control-word: No Encapsulation:
VLAN Qin-Q and VCI Interworking
Incoming label: 300192, Outgoing label: 299776 Negotiated PW
status TLV: No
Local interface: ge-1/0/1.0, Status: Up, Encapsulation: VLAN
Flow Label Transmit: No, Flow Label Receive: No
```
Meaning  The command output displays the Layer 2 virtual circuits from Router2 to its neighbors.

Related Documentation
- ATM-To-Ethernet Interworking on ATM MICs on page 267
- Example: Configuring ATM-to-Ethernet Interworking on ATM MIC on page 275
PART 2

Special Router Interfaces

- Configuring Discard Interfaces on page 289
- Configuring IP Demultiplexing Interfaces on page 293
- Configuring the Loopback Interface on page 309
CHAPTER 6

Configuring Discard Interfaces

- Discard Interfaces Overview on page 289
- Configuring Discard Interfaces on page 290

Discard Interfaces Overview

The discard interface dsc is not a physical interface, but a virtual interface that discards packets.

The following sections explain discard interfaces in detail:

- Understanding Discard Interfaces on page 289
- Guidelines to Follow When Configuring a Discard Interface on page 289

Understanding Discard Interfaces

The discard interface allows you to identify the ingress point of a denial-of-service (DoS) attack. When your network is under attack, the target host IP address is identified, and the local policy forwards attacking packets to the discard interface. When traffic is routed out of the discard interface, the traffic is silently discarded.

The discard interface allows you to protect a network from DoS attacks by identifying the target IP address that is being attacked and configuring a policy to forward all packets to a discard interface. All packets forwarded to the discard interface are dropped. See Example: Forwarding Packets to the Discard Interface.

You can configure the inet family protocol on the discard interface, which allows you to apply an output filter to the interface. If you apply an output filter to the interface, the action specified by the filter is executed before the traffic is discarded.

Once you configure a discard interface, you must then configure a local policy to forward attacking traffic to the discard interface.

Guidelines to Follow When Configuring a Discard Interface

Keep the following guidelines in mind when configuring the discard interface:

- Only the logical interface unit 0 is supported.
- The filter and address statements are optional.
Although you can configure an input filter and a filter group, these configuration statements have no effect because traffic is not transmitted from the discard interface.

- The discard interface does not support class of service (CoS).

Related Documentation
- Configuring Discard Interfaces on page 290
- Example: Forwarding Packets to the Discard Interface

Configuring Discard Interfaces

The discard (dsc) interface is not a physical interface, but a virtual interface that discards packets. You can configure one discard interface. When your network is under attack, the target host IP address is identified, and the local policy forwards attacking packets to the discard interface. Traffic routed out of the discard interface is silently discarded.

The following sections explain how to configure a discard interface:

- Configuring and Usage of Discard Interface on page 290
- Configure an Output Filter with Output policy on page 291

Configuring and Usage of Discard Interface

To configure a discard interface:

1. In configuration mode, go to the [edit interfaces] hierarchy level.

   [edit]
   user@host# edit interfaces

2. Configure the discard interface. Note that you must use 'dsc' to configure discard interface and ensure that there is no discard interface already configured.

   [edit interfaces]
   user@host# edit dsc

3. Configure the logical interface and the protocol family.

   [edit interfaces dsc]
   user@host# edit unit 0 family family

4. If appropriate, apply an output filter to the discard interface.
   Input filters have no impact in this context.

   [edit interfaces dsc unit 0 family family]
   user@host# set filter output filter-name
5. Commit the configuration and go to the top of the hierarchy level.

[edit interfaces dsc unit 0 family family]
user@host# commit
user@host# top

**Configure an Output Filter with Output Policy**

You must configure an output policy to set up the community on the routes injected into the network.

To configure an output policy.

1. In configuration mode, go to the [edit policy-options] hierarchy level.

   [edit]
   user@host# edit policy-options

2. Configure a routing policy.

   [edit policy-options]
   user@host# edit policy-statement statement-name

3. Configure a policy term with a name.

   [edit policy-options policy-statement statement-name]
   user@host# edit term term-variable

4. Configure the list of prefix-lists of routes to match with a name.

   [edit policy-options policy-statement statement-name term term-variable]
   user@host# set from prefix-list name

5. Configure the action that is to be taken when the if and to conditions match with the then statement. In this case, configure the BGP community properties (set, add, and delete) associated with a route.

   [edit policy-options policy-statement statement-name term term-variable]
   user@host# set then community (set | add | delete) community-name

6. Commit the configuration and go to the top of the hierarchy level.

   [edit interfaces dsc unit 0 family family]
   user@host# commit
   user@host# top
Related Documentation

- Discard Interfaces Overview on page 289
CHAPTER 7

Configuring IP Demultiplexing Interfaces

- Demultiplexing Interface Overview on page 293
- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301

Demultiplexing Interface Overview

Demultiplexing (demux) interfaces are logical interfaces that share a common, underlying interface. You can create logical subscriber interfaces using static or dynamic demultiplexing interfaces. In addition, you can use IP demultiplexing interfaces or VLAN demultiplexing interfaces when creating logical subscriber interfaces.

Demux interfaces are supported on M120 or MX Series routers only.

Demux interfaces support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.

NOTE: You can also configure demux interfaces dynamically. For information about how to configure dynamic IP demux or dynamic VLAN demux interfaces, see Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles or Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles.

To configure static demux interfaces, see “Configuring a VLAN Demultiplexing Interface” on page 301 and “Configuring an IP Demultiplexing Interface” on page 296.

- IP Demux Interface Overview on page 293
- VLAN Demux Interface Overview on page 294
- Guidelines to Remember When Configuring A Demux Interface on page 294
- MAC Address Validation on Static Demux Interfaces on page 295

IP Demux Interface Overview

IP demux interfaces use the IP source address or IP destination address to demultiplex received packets when the subscriber is not uniquely identified by a Layer 2 circuit.
To determine which IP demux interface to use, the destination or source prefix is matched against the destination or source address of packets that the underlying interface receives. The underlying interface family type must match the demux interface prefix type.

VLAN Demux Interface Overview

VLAN demux interfaces use the VLAN ID to demultiplex received packets when the subscriber is not uniquely identified. A VLAN demux interface uses an underlying logical interface to receive packets.

To determine which VLAN demux interface to use, the VLAN ID is matched against that which the underlying interface receives.

NOTE: VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other MPCs in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

Guidelines to Remember When Configuring A Demux Interface

Keep the following guidelines in mind when configuring the demux interface:

- Demux interfaces are supported on M120 or MX Series routers only.
- Only demux0 is supported. If you configure another demux interface, such as demux1, the configuration commit fails.
- You can configure only one demux0 interface per chassis, but you can define logical demux interfaces on top of it (for example, demux0.1, demux0.2, and so on).
- If the address in a received packet does not match any demux prefix, the packet is logically received on the underlying interface. For this reason, the underlying interface is often referred to as the primary interface.

- Points to Remember When Configuring an IP Demux Interface on page 295
- Points to Remember When Configuring a VLAN Demux Interface on page 295
Points to Remember When Configuring an IP Demux Interface

In addition to the guidelines in “Guidelines to Remember When Configuring A Demux Interface” on page 294, the following guidelines are to be noted when configuring an IP demux interface:

- You must associate demux interfaces with an underlying logical interface.

**NOTE:** IP demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.

- The demux underlying interface must reside on the same logical system as the demux interfaces that you configure over it.
- IP demux interfaces currently supports the Internet Protocol version 4 (IPv4) suite inet and Internet Protocol version 6 (IPv6) suite inet6 family types.
- You can configure more than one demux prefix for a given demux unit. However, you cannot configure the exact same demux prefix on two different demux units with the same underlying interface.
- You can configure overlapping demux prefixes on two different demux units with the same underlying prefix. However, under this configuration, best match rules apply (in other words, the most specific prefix wins).

Points to Remember When Configuring a VLAN Demux Interface

In addition to the guidelines in “Guidelines to Remember When Configuring A Demux Interface” on page 294, the following guidelines are to be noted when configuring a VLAN demux interface:

- You must associate VLAN demux interfaces with an underlying logical interface.

**NOTE:** VLAN demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.

- The demux underlying interface must reside on the same logical system as the demux interfaces that you configure over it.
- VLAN demux interfaces currently supports the Internet Protocol version 4 (IPv4) suite inet and Internet Protocol version 6 (IPv6) suite inet6 family types.

MAC Address Validation on Static Demux Interfaces

MAC address validation enables the router to validate that received packets contain a trusted IP source and an Ethernet MAC source address.
MAC address validation is supported on static demux interfaces on MX Series routers only.

There are two types of MAC address validation that you can configure:

- **Loose** on page 296
- **Strict** on page 296

**Loose**

Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not support the MAC address of the tuple.

Continues to forward packets when the source address of the incoming packet does not match any of the trusted IP addresses.

**Strict**

Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.

**Related Documentation**

- Associating VLAN IDs to VLAN Demux Interfaces
- Binding VLAN IDs to Logical Interfaces
- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
- Subscriber Interfaces and Demultiplexing Overview

**Configuring an IP Demultiplexing Interface**

Demultiplexing (demux) interfaces are logical interfaces that share a common, underlying interface. You can configure IP demultiplexing interfaces or VLAN demultiplexing interfaces.

To configure an IP demux interface, you must configure the demux prefixes that are used by the underlying interface and then configure the IP demultiplexing interface as explained in the following tasks:

1. Configuring an IP Demux Underlying Interface on page 297
2. Configuring the IP Demux Interface on page 298
3. Configuring MAC Address Validation on Static IP Demux Interfaces on page 300
Configuring an IP Demux Underlying Interface

An IP demux interface uses an underlying logical interface to receive packets. To determine which IP demux interface to use, the destination or source prefix is matched against the destination or source address of packets that the underlying interface receives. The underlying interface family type must match the demux interface prefix type.

NOTE: IP demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.

To configure a logical interface as an IP demux underlying interface with demux source:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

   [edit]
   user@host# edit interfaces

2. Configure the interface as fe-x/y/z and the logical interface with the unit statement. Note that IP demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces. In this procedure, we show a Fast Ethernet interface as an example.

   [edit interfaces]
   user@host# edit fe-x/y/z unit logical-unit-number

3. Configure the logical demux source family type on the IP demux underlying interface as inet or inet6, or both.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set demux-source (inet | inet6)

   or

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set demux-source [inet inet6]

4. (Optional) To improve datapath performance for DHCPv4 subscribers, specify that only subscribers with 32-bit prefixes are allowed to come up on the interface.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set host-prefix-only

NOTE: This step requires that you specify the demux-source as only inet. A commit error occurs if you specify only inet6 or both inet and inet6.
5. Save the configuration and move to top of the hierarchy level.

```
[edit interfaces fe-x/y/z unit logial-unit-number]
user@host# commit
user@host# top
```

To configure a logical interface as an IP demux underlying interface with demux destination:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

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

2. Configure the interface as fe-x/y/z and the logical interface with the unit statement. Note that IP demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.

```
[edit interfaces]
user@host# edit fe-x/y/z unit logical-unit-number unit logical-unit-number
```

3. Configure the logical demux destination family type on the IP demux underlying interface as inet or inet6.

```
[edit interfaces fe-x/y/z unit logical-unit-number]
user@host# set demux-destination (inet | inet6)
```

4. Save the configuration and move to top of the hierarchy level.

```
[edit interfaces fe-x/y/z unit logical-unit-number]
user@host# commit
user@host# top
```

### Configuring the IP Demux Interface

You can configure one or more logical demux source prefixes or destination prefixes after specifying an underlying interface for the static demux interface to use. This underlying interface must reside on the same logical system as the demux interface.

You configure demux prefixes for use by the underlying interface. The demux prefixes can represent individual hosts or networks. For a given demux interface unit, you can configure either demux source or demux destination prefixes but not both.

You can choose not to configure a demux source or demux destination prefix. This type of configuration results in a transmit-only interface.

To configure the IP demux interface with source prefix:

1. In configuration mode, go to the [edit interfaces] hierarchy level:
[edit]
user@host# edit interfaces

2. Configure the interface as a logical demux interface (for example, demux0 interface) and configure the logical interface with the unit statement.

NOTE: You can configure only one demux0 interface per chassis, but you can define logical demux interfaces on top of it (for example, demux0.1, demux0.2, and so on).

[edit interfaces]
user@host# edit demux0 unit logical-unit-number

3. Configure the underlying interface on which the demux interface is running under the demux-options statement.

[edit interfaces demux0 unit logical-unit-number]
user@host# set demux-options underlying-interface interface-name

4. Configure the protocol family.

[edit interfaces demux0 unit logical-unit-number]
user@host# edit family family

5. Configure one or more logical demux source prefixes (IP address). The prefixes are matched against the source address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

[edit interfaces demux0 unit logical-unit-number family family]
user@host# set demux-source source-prefix

6. Save the configuration and move to top of the hierarchy level.

[edit interfaces demux0 unit logical-unit-number family family]
user@host# commit
user@host# top

To configure the IP demux interface with destination prefix:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

[edit]
user@host# edit interfaces
2. Configure the interface as a logical demux interface (for example, demux0 interface) and configure the logical interface with the unit statement.

   ![NOTE:](image) You can configure only one demux0 interface per chassis, but you can define logical demux interfaces on top of it (for example, demux0.1, demux0.2, and so on).

   

   ```
   [edit interfaces]
   user@host# edit demux0 unit logical-unit-number
   ```

3. Configure the underlying interface on which the demux interface is running under the demux-options statement.

   ```
   [edit interfaces demux0 unit logical-unit-number]
   user@host# set demux-options underlying-interface interface-name
   ```

4. Configure the protocol family.

   ```
   [edit interfaces demux0 unit logical-unit-number]
   user@host# edit family family
   ```

5. Configure one or more logical demux destination prefixes. The prefixes are matched against the destination address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

   ```
   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# set demux-destination destination-prefix
   ```

6. Save the configuration and move to top of the hierarchy level.

   ```
   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# commit
   user@host# top
   ```

### Configuring MAC Address Validation on Static IP Demux Interfaces

MAC address validation enables the router to validate that received packets contain a trusted IP source and an Ethernet MAC source address.

To configure MAC address validation for an IP demux interface:

1. In configuration mode, go to the `edit interfaces demux0 unit logical-unit-number` hierarchy level:

   ```
   [edit]
   ```
2. Configure the protocol family for the interface.

   
   [edit interfaces demux0 unit logical-unit-number]
   user@host# edit family family

3. Configure the `mac-validate` statement to validate source MAC address with loose or strict options.

   
   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# set mac-validate (loose | strict)

4. Save the configuration and move to top of the hierarchy level.

   
   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# commit
   user@host# top

**Related Documentation**

- Configuring a VLAN Demultiplexing Interface on page 301
- Demultiplexing Interface Overview on page 293

**Configuring a VLAN Demultiplexing Interface**

Demultiplexing (demux) interfaces are logical interfaces that share a common, underlying interface. You can configure IP demultiplexing interfaces or VLAN demultiplexing interfaces.

To configure a VLAN demux interface, you must configure the demux prefixes that are used by the underlying interface and then configure the VLAN demultiplexing interface as explained by the following tasks:

1. Configuring a VLAN Demux Underlying Interface on page 301
2. Configuring the VLAN Demux Interface on page 303
3. Configuring MAC Address Validation on Static VLAN Demux Interfaces on page 305
4. Verifying a Demux Interface Configuration on page 306

**Configuring a VLAN Demux Underlying Interface**

A VLAN demux interface uses an underlying logical interface to receive packets. To determine which VLAN demux interface to use, the VLAN ID is matched against that which the underlying interface receives.
NOTE: VLAN demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.

VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other MPCs in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

To configure a logical interface as a VLAN demux underlying interface with demux source:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

   [edit]
   user@host# edit interfaces

2. Configure the interface as fe-x/y/z and the logical interface with the unit option.

   [edit interfaces]
   user@host# edit fe-x/y/z unit logical-unit-number unit logical-unit-number

3. Configure the VLAN ID. The VLAN ID is used to determine which VLAN demux interface to use, that is the VLAN ID is matched against that which the underlying interface receives.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set vlan-id number

4. Configure the logical demux source family type on the VLAN demux underlying interface as inet or inet6.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set demux-source (inet | inet6)

5. Save the configuration and move to top of the hierarchy level.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# commit
   user@host# top

To configure a logical interface as a VLAN demux underlying interface with demux destination:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

   [edit]
2. Configure the interface as fe-x/y/z and the logical interface with the unit option.

   [edit interfaces]
   user@host# edit fe-x/y/z unit logical-unit-number unit logical-unit-number

3. Configure the VLAN ID. The VLAN ID is used to determine which VLAN demux interface to use, that is the VLAN ID is matched against that which the underlying interface receives.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set vlan-id number

4. Configure the logical demux destination family type on the VLAN demux underlying interface as inet or inet6.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# set demux-destination (inet | inet6)

5. Save the configuration and move to top of the hierarchy level.

   [edit interfaces fe-x/y/z unit logical-unit-number]
   user@host# commit
   user@host# top

### Configuring the VLAN Demux Interface

You can configure one or more logical demux source prefixes or destination prefixes after specifying an underlying interface for the static demux interface to use. This underlying interface must reside on the same logical system as the demux interface.

You configure demux prefixes for use by the underlying interface. The demux prefixes can represent individual hosts or networks. For a given demux interface unit, you can configure either demux source prefix or demux destination prefixes but not both.

You can choose not to configure a demux source prefix or a demux destination prefix. This type of configuration results in a transmit-only interface.

To configure VLAN demux interface with demux source prefix:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

   [edit]
   user@host# edit interfaces
2. Configure the interface as a logical demux interface (for example, demux0 interface) and configure the logical interface with the unit statement.

   NOTE: You can configure only one demux0 interface per chassis, but you can define logical demux interfaces on top of it (for example, demux0.1, demux0.2, and so on).

   ```
   [edit interfaces]
   user@host# edit demux0 unit logical-unit-number
   ```

3. Configure the underlying interface on which the demux interface is running under the demux-options statement.

   ```
   [edit interfaces demux0 unit logical-unit-number]
   user@host# set demux-options underlying-interface interface-name
   ```

4. Configure the protocol family for the interface.

   ```
   [edit interfaces demux0 unit logical-unit-number]
   user@host# edit family family
   ```

5. Configure one or more logical demux source prefixes. The prefixes are matched against the source address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

   ```
   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# set demux-source source-prefix
   ```

6. Save the configuration and move to top of the hierarchy level.

   ```
   [edit interfaces demux0 unit logical-unit-number]
   user@host# commit
   user@host# top
   ```

To configure VLAN demux interface with demux destination prefix:

1. In configuration mode, go to the [edit interfaces] hierarchy level:

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

2. Configure the interface as a logical demux interface (for example, demux0 interface) and configure the logical interface with the unit statement.
NOTE: You can configure only one demux0 interface per chassis, but you can define logical demux interfaces on top of it (for example, demux0.1, demux0.2, and so on).

```
[edit interfaces]
user@host# edit demux0 unit logical-unit-number
```

3. Configure the underlying interface on which the demux interface is running under the `demux-options` statement.

```
[edit interfaces demux0 unit logical-unit-number]
user@host# set demux-options underlying-interface interface-name
```

4. Configure the protocol family for the interface.

```
[edit interfaces demux0 unit logical-unit-number]
user@host# edit family family
```

5. Configure one or more logical demux destination prefixes. The prefixes are matched against the destination address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

```
[edit interfaces demux0 unit logical-unit-number family family]
user@host# set demux-destination destination-prefix
```

6. Save the configuration and move to top of the hierarchy level.

```
[edit interfaces demux0 unit logical-unit-number]
user@host# commit
user@host# top
```

**Configuring MAC Address Validation on Static VLAN Demux Interfaces**

MAC address validation enables the router to validate that received packets contain a trusted IP source and an Ethernet MAC source address.

To configure MAC address validation for a VLAN demux interface:

1. In configuration mode, go to the `[edit interfaces demux0 unit logical-unit-number]` hierarchy level:

```
[edit]
user@host# edit interfaces demux0 unit logical-unit-number
```
2. Configure the protocol family for the interface.

   [edit interfaces demux0 unit logical-unit-number]
   user@host# edit family family

3. Configure the `mac-validate` statement to validate source MAC address with loose or strict options.

   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# set mac-validate (loose | strict)

4. Save the configuration and move to top of the hierarchy level.

   [edit interfaces demux0 unit logical-unit-number family family]
   user@host# commit
   user@host# top

**Verifying a Demux Interface Configuration**

**Purpose**  
Check the configuration of a demux interface and its underlying interface when the following are configured:

- Two VLANs are configured, where each VLAN consists of two IP demux interfaces.
- One VLAN demultiplexes based on the source address.
- The other VLAN demultiplexes based on the destination address.

**Action**  
From configuration mode on the MX Series router, run the `show interfaces fe-0/0/0` and `show interfaces demux0` configuration mode commands.

```
user@host> show interfaces fe-0/0/0

vlan-tagging;
unit 100 {
  vlan-id 100;
  demux-source inet; # Enable demux of inet prefixes
  family inet {
    address 10.1.1.1/24;
    filter {
      input vlan1-primary-in-filter;
      output vlan1-primary-out-filter;
    }
    mac-validate loose;
  }
}
unit 200 {
  vlan-id 200;
  demux-destination inet; # Enable demux of inet using destination addresses
  family inet {
    address 20.1.1.1/24;
  }
```
unit 300 {
    vlan-id 300;
    demux-source inet; # Enable demux of inet using source addresses
    family inet {
        address 20.1.2.1/24;
    }
}

user@host> show interfaces demux0

unit 101 {
    description vlan1-sub1;
    demux-options {
        underlying-interface fe-0/0/0.100;
    }
    family inet {
        demux-source 10.1.1.0/24;
        filter {
            input vlan1-sub1-in-filter;
            output vlan1-sub1-out-filter;
        }
        mac-validate loose;
    }
}
unit 102 {
    description vlan1-sub2;
    demux-options {
        underlying-interface fe-0/0/0.100;
    }
    family inet {
        demux-source {
            10.1.0.0/16;
            10.2.1.0/24;
        }
        filter {
            input vlan1-sub2-in-filter;
            output vlan1-sub2-out-filter;
        }
        mac-validate loose;
    }
}
unit 202 {
    description vlan2-sub2;
    demux-options {
        underlying-interface fe-0/0/0.200;
    }
    family inet {
        demux-destination 100.1.2.0/24;
    }
}
unit 302 {
    description vlan2-sub2;
    demux-options {
        underlying-interface fe-0/0/0.300;
    }
    family inet {
        demux-source 100.1.2.0/24;
    }
Related Documentation

- Configuring an IP Demultiplexing Interface on page 296
- Demultiplexing Interface Overview on page 293
Understanding the Loopback Interface

The loopback address (lo0) has several uses, depending on the particular Junos feature being configured. It can perform the following functions:

- **Device identification**—The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address never changes.

  When you ping an individual interface address, the results do not always indicate the health of the device. For example, a subnet mismatch in the configuration of two endpoints on a point-to-point link makes the link appear to be inoperable. Pinging the interface to determine whether the device is online provides a misleading result. An interface might be unavailable because of a problem unrelated to the device’s configuration or operation.

- **Routing information**—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as `ping mpls` require a loopback address to function correctly.

- **Packet filtering**—Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

The Internet Protocol (IP) specifies a loopback network with the (IPv4) address 127.0.0.0/8. Most IP implementations support a loopback interface (lo0) to represent the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6. The standard domain name for the address is `localhost`.

The device also includes an internal loopback address (lo0.16384). The internal loopback address is a particular instance of the loopback address with the logical unit number 16384. Junos OS creates the loopback interface for the internal routing instance. This interface prevents any filter on lo0.0 from disrupting internal traffic.
Loopback Interface Configuration

- Configuring the Loopback Interface on page 310
- Example: Configuring Two Addresses on the Loopback Interface with Host Routes on page 311
- Example: Configuring Two Addresses on the Loopback Interface with Subnetwork Routes on page 311
- Example: Configuring an IPv4 and an IPv6 Address on the Loopback Interface with Subnetwork Routes on page 312

Configuring the Loopback Interface

When specifying the loopback address, do not include a destination prefix. Also, in most cases, do not specify a loopback address on any unit other than unit 0.

NOTE: For Layer 3 virtual private networks (VPNs), you can configure multiple logical units for the loopback interface. This allows you to configure a logical loopback interface for each virtual routing and forwarding (VRF) routing instance. For more information, see the Junos OS VPNs Library for Routing Devices.

For some applications, such as SSL for Junos XML protocol, the address for the interface lo0.0 must be 127.0.0.1.

You can configure loopback interfaces using a subnetwork address for both inet and inet6 address families. Many protocols require a subnetwork address as their source address. Configuring a subnetwork loopback address as a donor interface enables these protocols to run on unnumbered interfaces.

If you configure the loopback interface, it is automatically used for unnumbered interfaces. If you do not configure the loopback interface, the router chooses the first interface to come online as the default. If you configure more than one address on the loopback interface, we recommend that you configure one to be the primary address to ensure that it is selected for use with unnumbered interfaces. By default, the primary address is used as the source address when packets originate from the interface.

On the router, you can configure one physical loopback interface, lo0, and one or more addresses on the interface.

1. To configure the physical loopback interface, include the following statements at the [edit interfaces] hierarchy level:

    [edit interfaces]
    lo0 {
        unit 0 {
    

Example: Configuring Two Addresses on the Loopback Interface with Host Routes

To configure two addresses on the loopback interface with host routes:

```
[edit]
user@host# edit interfaces lo0 unit 0 family inet
[edit interfaces lo0 unit 0 family inet]
user@host# set address 172.16.0.1
[edit interfaces lo0 unit 0 family inet]
user@host# set address 10.0.0.1
[edit interfaces lo0 unit 0 family inet]
user@host# top
[edit]
user@host# show
interfaces {
lo0 {
  unit 0 {
    family inet {
      10.0.0.1;
      127.0.0.1;
      172.16.0.1;
    }
  }
}
}
```

Example: Configuring Two Addresses on the Loopback Interface with Subnetwork Routes

To configure two addresses on the loopback interface with subnetwork routes:

```
[edit]
user@host# edit interfaces lo0 unit 0 family inet
[edit interfaces lo0 unit 0 family inet]
user@host# set address 192.16.0.1/24
[edit interfaces lo0 unit 0 family inet]
user@host# set address 10.2.0.1/16
[edit interfaces lo0 unit 0 family inet]
user@host# top
[edit]
user@host# show
interfaces {
```
Example: Configuring an IPv4 and an IPv6 Address on the Loopback Interface with Subnetwork Routes

To configure an IPv4 and an IPv6 address on the loopback interface with subnetwork routes:

```
[edit]
user@host# edit interfaces lo0 unit 0 family inet
[edit interfaces lo0 unit 0 family inet]
user@host# set address 192.16.0.1/24
[edit interfaces lo0 unit 0 family inet]
user@host# up
[edit interfaces lo0 unit 0 family]
user@host# edit interfaces lo0 unit 0 family inet6
[edit interfaces lo0 unit 0 family inet6]
user@host# set address 3ffe::1:200:f8ff:fe75:50df/64
[edit interfaces lo0 unit 0 family inet6]
user@host# top
[edit]
user@host# show
interfaces {
  lo0 {
    unit 0 {
      family inet {
        10.2.0.1/16;
        127.0.0.1/32;
        192.16.0.1/24;
      }
    }
    family inet6 {
      3ffe::1:200:f8ff:fe75:50df/64;
    }
  }
}
```

Related Documentation

- Junos OS VPNs Library for Routing Devices
- Configuring an Unnumbered Interface on page 202
- Configuring the Interface Address on page 191
PART 3

Serial Interfaces

- Serial Interfaces Overview on page 315
- Configuring Serial Interfaces on page 317
Serial Interfaces Overview

Devices that communicate over a serial interface are divided into two classes: data terminal equipment (DTE) and data circuit-terminating equipment (DCE). Juniper Networks Serial Physical Interface Cards (PICs) have two ports per PIC and support full-duplex data transmission. These PICs support DTE mode only. On the Serial PIC, you can configure three types of serial interfaces:

- **EIA-530**—An Electronics Industries Alliance (EIA) standard for the interconnection of DTE and DCE using serial binary data interchange with control information exchanged on separate control circuits.
- **V.35**—An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe.
- **X.21**—An ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

The following standards apply to serial interfaces:

- TIA/EIA Standard 530, *High-Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment*, defines the signals on the cable and specifies the connector at the end of the cable.
- TIA/EIA Standard 232, *Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, describes the physical interface and protocol for serial data communication.
- ITU-T Recommendation V.35, *Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits*. Note that the Juniper Networks Serial PIC supports V.35 interfaces with speeds higher than 48 kilobits per second.

There are no serial interface-specific logical properties. For information about general logical properties that you can configure, see *Configuring Logical Interface Properties*. This
support on serial interfaces is the same as the existing LFI and MLPPP support on T1 and E1 interfaces.

**Related Documentation**
- Example: Physical Interface Configuration Statements for Serial Interfaces on page 317
- Configuring the Serial Line Protocol on page 318
- Configuring the Serial Clocking Mode on page 322
- Configuring the Serial Signal Handling on page 324
- Configuring the Serial DTR Circuit on page 327
- Configuring Serial Signal Polarities on page 327
- Configuring Serial Loopback Capability on page 328
- Configuring Serial Line Encoding on page 330
CHAPTER 10

Configuring Serial Interfaces

- Example: Physical Interface Configuration Statements for Serial Interfaces on page 317
- Configuring the Serial Line Protocol on page 318
- Configuring the Serial Clocking Mode on page 322
- Configuring the Serial Signal Handling on page 324
- Configuring the Serial DTR Circuit on page 327
- Configuring Serial Signal Polarities on page 327
- Configuring Serial Loopback Capability on page 328
- Configuring Serial Line Encoding on page 330
- Specifying a USB Modem Interface on J Series Routers on page 331

Example: Physical Interface Configuration Statements for Serial Interfaces

To configure serial physical interface properties, include the `serial-options` statement at the [edit interfaces se-fpc/pic/port] hierarchy level.

```
[edit interfaces se-fpc/pic/port]
serial-options {
  clock-rate rate;
  clocking-mode (dce | internal | loop);
  control-polarity (negative | positive);
  cts-polarity (negative | positive);
  dcd-polarity (negative | positive);
  dce-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dsr-polarity (negative | positive);
  dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
  }
```

Copyright © 2019, Juniper Networks, Inc.
Configuring the Serial Line Protocol

- Configuring the Serial Line Protocol on page 318
- Serial Interface Default Settings on page 318

Configuring the Serial Line Protocol

By default, serial interfaces use the EIA-530 line protocol. You can configure each port on the PIC independently to use one of the following line protocols:

- EIA-530
- V.35
- X.21

To configure the serial line protocol:

1. Include the `line-protocol` statement, specifying the `eia530`, `v.35`, or `x.21` option:

```
line-protocol protocol;
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

For more information about serial interfaces, see the following sections:

Serial Interface Default Settings

- Serial Interface Default Settings on page 319
- Invalid Serial Interface Statements on page 320
Serial Interface Default Settings

- EIA-530 Interface Default Settings on page 319
- V.35 Interface Default Settings on page 319
- X.21 Interface Default Settings on page 320

**EIA-530 Interface Default Settings**

If you do not include the `line-protocol` statement or if you explicitly configure the default EIA-530 line protocol, the default settings are as follows:

```plaintext
dce-options | dte-options {
  cts normal;
  dcd normal;
  dsr normal;
  dtr normal;
  rts normal;
  tm normal;
}
clock-rate 16.384mhz;
clocking-mode loop;
cts-polarity positive;
dcd-polarity positive;
rsr-polarity positive;
dtr-circuit balanced;
dtr-polarity positive;
encoding nrz;
rts-polarity positive;
trm-polarity positive;
```

**NOTE:** On M Series routers, you can set the DCE clocking mode for EIA-530 interfaces and commit. An error message is not displayed and the CLI is not blocked.

You can include the `line-protocol` statement at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

**V.35 Interface Default Settings**

If you include the `line-protocol v.35` statement, the default settings are as follows:

```plaintext
dce-options | dte-options {
  cts normal;
  dcd normal;
  dsr normal;
  dtr normal;
  rts normal;
}
```
clock-rate 16.384mhz;
clocking-mode loop;
ccts-polarity positive;
dcd-polarity positive;
dsr-polarity positive;
dtr-circuit balanced;
dtr-polarity positive;
encoding nrz;
rts-polarity positive;

You can include the line-protocol statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

**X.21 Interface Default Settings**

If you include the line-protocol x.21 statement, the default settings are as follows:

```
dce-options | dte-options {
    control-signal normal;
    indication normal;
}
clock-rate 16.384mhz;
clocking-mode loop;
control-polarity positive;
encoding nrz;
indication-polarity positive;
```

You can include the line-protocol statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

**Invalid Serial Interface Statements**

The following sections show the invalid configuration statements for each type of serial interface. If you include the following statements in the configuration, an error message indicates the location of the error and the configuration is not activated.

- Invalid EIA-530 Interface Statements on page 320
- Invalid V.35 interface Statements on page 321
- Invalid X.21 Interface Statements on page 321

**Invalid EIA-530 Interface Statements**

If you do not include the line-protocol statement or if you explicitly configure the default EIA-530 line protocol, the following statements are invalid:

```
dce-options | dte-options {
    control-signal (assert | de-assert | normal);
    indication (ignore | normal | require);
```
You can include the **line-protocol** statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

### Invalid V.35 Interface Statements

If you include the **line-protocol v.35** statement, the following statements are invalid:

```plaintext
  dce-options | dte-options {
    control-signal (assert | de-assert | normal);
    indication (ignore | normal | require);
    tm (ignore | normal | require);
  }
  control-polarity (negative | positive);
  indication-polarity (negative | positive);
  loopback (dce-local | dce-remote);
  tm-polarity (negative | positive);
```

You can include the **line-protocol** statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

### Invalid X.21 Interface Statements

If you include the **line-protocol x.21** statement, the following statements are invalid:

```plaintext
  dce-options | dte-options {
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr (assert | de-assert | normal);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
    }
  clocking-mode (dce | internal);
  cts-polarity (negative | positive);
  dce-polarity (negative | positive);
  dsr-polarity (negative | positive);
  dtr-circuit (balanced | unbalanced);
  dtr-polarity (negative | positive);
  loopback (dce-local | dce-remote);
  rts-polarity (negative | positive);
  tm-polarity (negative | positive);
```

You can include the **line-protocol** statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
Configuring the Serial Clocking Mode

By default, serial interfaces use loop clocking mode. For EIA-530 and V.35 interfaces, you can configure each port on the PIC independently to use loop, DCE, or internal clocking mode. For X.21 interfaces, only loop clocking mode is supported.

The three clocking modes work as follows:

- **Loop clocking mode**—Uses the DCE’s RX clock to clock data from the DCE to the DTE.
- **DCE clocking mode**—Uses the TXC clock, which is generated by the DCE specifically to be used by the DTE as the DTE’s transmit clock.
- **Internal clocking mode**—Also known as line timing, uses an internally generated clock. You can configure the speed of this clock by including the `clock-rate` statement at the `[edit interfaces se-fpc/pic/port serial-options]` or `[edit interfaces se-fpc/pic/port dte-options]` hierarchy levels. For more information about the DTE clock rate, see “Configuring the DTE Clock Rate” on page 323.

Note that DCE clocking mode and loop clocking mode use external clocks generated by the DCE.

Figure 21 on page 322 shows the clock sources of loop, DCE, and internal clocking modes.

Figure 21: Serial Interface Clocking Mode

To configure the clocking mode of a serial interface, include the `clocking-mode` statement:
clocking-mode \(\text{(dce | internal | loop)}\);

You can include this statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

### Inverting the Serial Interface Transmit Clock

When an externally timed clocking mode (DCE or loop) is used, long cables might introduce a phase shift of the DTE-transmitted clock and data. At high speeds, this phase shift might cause errors. Inverting the transmit clock corrects the phase shift, thereby reducing error rates.

By default, the transmit clock is not inverted. To invert the transmit clock, include the `transmit-clock invert` statement:

```
transmit-clock invert;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

### Configuring the DTE Clock Rate

By default, the serial interface has a clock rate of 16.384 MHz. For EIA-530 and V.35 interfaces with internal clocking mode configured, you can configure the clock rate.

To configure the clock rate, include the `clock-rate` statement:

```
clock-rate rate;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

You can configure the following interface speeds:

- 2.048 MHz
- 2.341 MHz
- 2.731 MHz
- 3.277 MHz
- 4.096 MHz
- 5.461 MHz
• 8.192 MHz
• 16.384 MHz

Although the serial interface is intended for use at the default rate of 16.384 MHz, you might need to use a slower rate if any of the following conditions prevail:

• The interconnecting cable is too long for effective operation.
• The interconnecting cable is exposed to an extraneous noise source that might cause an unwanted voltage in excess of +1 volt measured differentially between the signal conductor and circuit common at the load end of the cable, with a 50-ohm resistor substituted for the generator.
• You need to minimize interference with other signals.
• You need to invert signals.

For detailed information about the relationship between signaling rate and interface cable distance, see the following standards:

• EIA-422-A, Electrical Characteristics of Balanced Voltage Digital Interface Circuits
• EIA-423-A, Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits

Related Documentation
• Serial Interfaces Overview on page 315

Configuring the Serial Signal Handling

By default, normal signal handling is enabled for all signals. For each signal, the normal option applies to the normal signal handling for that signal, as defined by the following standards:

• TIA/EIA Standard 530
• ITU-T Recommendation V.35
• ITU-T Recommendation X.21

Table 24 on page 324 shows the serial interface modes that support each signal type.

Table 24: Signal Handling by Serial Interface Type

<table>
<thead>
<tr>
<th>Signal</th>
<th>Serial Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>From-DCE signals</td>
<td></td>
</tr>
<tr>
<td>Clear to send (CTS)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Data carrier detect (DCD)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Data set ready (DSR)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Indication</td>
<td>X.21 only</td>
</tr>
</tbody>
</table>
### Table 24: Signal Handling by Serial Interface Type (continued)

<table>
<thead>
<tr>
<th>Signal</th>
<th>Serial Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test mode (TM)</td>
<td>EIA-530 only</td>
</tr>
<tr>
<td>To-DCE signals</td>
<td></td>
</tr>
<tr>
<td>Control signal</td>
<td>X.21 only</td>
</tr>
<tr>
<td>Data transfer ready (DTR)</td>
<td>EIA-530 and V.35</td>
</tr>
<tr>
<td>Request to send (RTS)</td>
<td>EIA-530 and V.35</td>
</tr>
</tbody>
</table>

You configure serial interface signal characteristics by including the `dce-options` or `dte-options` statement:

```hll

dce-options | dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

For EIA-530 and V.35 interfaces, configure to-DCE signals by including the `dtr` and `rts` statements, specifying the `assert`, `de-assert`, or `normal` option:

```hll
dtr (assert | de-assert | normal);
rts (assert | de-assert | normal);
```

For X.21 interfaces, configure to-DCE signals by including the `control-signal` statement, specifying the `assert`, `de-assert`, or `normal` option:

```hll
control-signal (assert | de-assert | normal);
```

**Assertion** is when the positive side of a given signal is at potential high-level output voltage (Voh), while the negative side of the same signal is at potential low-level output voltage (Vol). **Deassertion** is when the positive side of a given signal is at potential Vol, while the negative side of the same signal is at potential Voh.
For the DTR signal, you can configure normal signal handling using the signal for automatic resynchronization by including the dtr statement, and specifying the auto-synchronize option:

```plaintext
dtr {
  auto-synchronize {
    duration milliseconds;
    interval seconds;
  }
}
```

The pulse duration of resynchronization can be from 1 through 1000 milliseconds. The offset interval for resynchronization can be from 1 through 31 seconds.

For EIA-530 and V.35 interfaces, configure from-DCE signals by including the cts, dcd, and dsr statements, specifying the ignore, normal, or require option:

```plaintext
ccts (ignore | normal | require);
dcd (ignore | normal | require);
dsr (ignore | normal | require);
```

For X.21 interfaces, configure from-DCE signals by including the indication statement, specifying the ignore, normal, or require option:

```plaintext
indication (ignore | normal | require);
```

For EIA-530 interfaces only, you can configure from-DCE test-mode (TM) signaling by including the tm statement, specifying the ignore, normal, or require option:

```plaintext
tm (ignore | normal | require);
```

To specify that the from-DCE signal must be asserted, include the require option in the configuration. To specify that the from-DCE signal must be ignored, include the ignore option in the configuration.

---

**NOTE:** For V.35 and X.21 interfaces, you cannot include the tm statement in the configuration.

For X.21 interfaces, you cannot include the cts, dcd, dsr, dtr, and rts statements in the configuration.

For EIA-530 and V.35 interfaces, you cannot include the control-signal and indication statements in the configuration.

For a complete list of serial options statements that are not supported by each serial interface mode, see “Invalid Serial Interface Statements” on page 320.

To return to the default normal signal handling, delete the require, ignore, assert, de-assert, or auto-synchronize statement from the configuration, as shown in the following example:
To explicitly configure normal signal handling, include the `control-signal` statement with the `normal` option:

```
control-signal normal;
```

You can configure the serial interface to ignore all control leads by including the `ignore-all` statement:

```
ignore-all;
```

You can include the `ignore-all` statement in the configuration only if you do not explicitly enable other signal handling options at the `[edit interfaces se-pim/0/port serial-options dce-options]` or `[edit interfaces se-fpc/pic/port serial-options dte-options]` hierarchy levels.

You can include the `control-signal`, `cts`, `dcd`, `dsr`, `dtr`, `indication`, `rts`, and `tm` statements at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options dte-options]`
- `[edit interfaces se-fpc/pic/port serial-options dte-options]`

### Configuring the Serial DTR Circuit

A balanced circuit has two currents that are equal in magnitude and opposite in phase. An unbalanced circuit has one current and a ground; if a pair of terminals is unbalanced, one side is connected to electrical ground and the other carries the signal. By default, the DTR circuit is balanced.

For EIA-530 and V.35 interfaces, configure the DTR circuit by including the `dtr-circuit` statement:

```
dtr-circuit (balanced | unbalanced);
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

### Configuring Serial Signal Polarities

Serial interfaces use a differential protocol signaling technique. Of the two serial signals associated with a circuit, the one referred to as the A signal is denoted with a plus sign, and the one referred to as the B signal is denoted with a minus sign; for example, DTR+ and DTR−. If DTR is low, then DTR+ is negative with respect to DTR−. If DTR is high, then DTR+ is positive with respect to DTR−.
By default, all signal polarities are positive. You can reverse this polarity on a Juniper Networks serial interface. You might need to do this if signals are miswired as a result of reversed polarities.

For EIA-530 and V.35 interfaces, configure signal polarities by including the `cts-polarity`, `dcd-polarity`, `dsr-polarity`, `dtr-polarity`, `rts-polarity`, and `tm-polarity` statements:

- `cts-polarity` (negative | positive);
- `dcd-polarity` (negative | positive);
- `dsr-polarity` (negative | positive);
- `dtr-polarity` (negative | positive);
- `rts-polarity` (negative | positive);
- `tm-polarity` (negative | positive);

You can include these statements at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

For X.21 interfaces, configure signal polarities by including the `control-polarity` and `indication-polarity` statements:

- `control-polarity` (negative | positive);
- `indication-polarity` (negative | positive);

You can include these statements at the following hierarchy levels:

- `[edit interfaces se-pim/0/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

### Configuring Serial Loopback Capability

From the router, remote line interface unit (LIU) loopback loops the TX (transmit) data and TX clock back to the router as RX (receive) data and RX clock. From the line, LIU loopback loops the RX data and RX clock back out the line as TX data and TX clock, as shown in Figure 22 on page 328.

*Figure 22: Serial Interface LIU Loopback*
DCE local and DCE remote control the EIA-530 interface-specific signals for enabling local and remote loopback on the link partner DCE. Local loopback is shown in Figure 23 on page 329.

**Figure 23: Serial Interface Local Loopback**

For EIA-530 interfaces, you can configure DCE local, DCE remote, local, and remote (LIU) loopback capability.

For V.35, you can configure remote LIU and local loopback capability. DCE local and DCE remote loopbacks are not supported on V.35 and X.21 interfaces. Local and remote loopbacks are not supported on X.21 interfaces.

To configure the loopback capability on a serial interface, include the `loopback` statement, specifying the `dce-local`, `dce-remote`, `local`, or `remote` option:

```
loopback mode;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces se-pim/O/port serial-options]`
- `[edit interfaces se-fpc/pic/port serial-options]`

To disable the loopback capability, remove the `loopback` statement from the configuration:

```
[edit]
user@host# delete interfaces se-fpc/pic/port serial-options loopback
```

You can determine whether there is an internal or external problem by checking the error counters in the output of the `show interface se-fpc/pic/port extensive` command:

```
user@host> show interfaces se-fpc/pic/port extensive
```

To Configure Serial Loopback Capability:

1. To determine the source of a problem, loop the packets on the local router, the local DCE, the remote DCE, and the remote line interface unit (LIU).
2. To do this, include the `no-keepalives` and `encapsulation cisco-hdlc` statements at the
[edit interfaces se-fpc/pic/port] hierarchy level, and the `loopback local` option at the
[edit interfaces se-pim/0/port serial-options] or [edit interfaces se-fpc/pic/port
serial-options] hierarchy level. With this configuration, the link stays up, so you can
loop ping packets to a remote router. The `loopback local` statement causes the
interface to loop within the PIC just before the data reaches the transceiver.

```
[edit interfaces]
se-1/0/0 {
  no-keepalives;
  encapsulation cisco-hdlc;
  serial-options {
    loopback local;
  }
  unit 0 {
    family inet {
      address 10.100.100.1/24;
    }
  }
}
```

Related Documentation

- Serial Interfaces Overview on page 315

Configuring Serial Line Encoding

By default, serial interfaces use non-return to zero (NRZ) line encoding. You can configure
non-return to zero inverted (NRZI) line encoding if necessary.

To have the interface use NRZI line encoding, include the `encoding` statement, specifying
the `nrzi` option:

```
encoding nrzi;
```

To explicitly configure the default NRZ line encoding, include the `encoding` statement,
specifying the `nrz` option:

```
encoding nrz;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces se-pim/0/port serial-options]
- [edit interfaces se-fpc/pic/port serial-options]

When setting the line encoding parameter, you must set the same value for paired ports.
Ports 0 and 1 must share the same value.
Specifying a USB Modem Interface on J Series Routers

The J Series routers contain two USB ports controlled by a single USB controller. One USB port can support USB devices, while the other one can act as a USB modem.

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 (dlIn) and the physical interface (umdo) to be bound together dynamically on a per-call basis.

The following dialer interface features are supported by the USB modem interface:

• Encapsulation PPP
• CoS
• NAT
• Interface statistics
• Packet capture
• GRE tunnel
• Stateful firewall
• Traffic sampling

To configure a USB modem interface, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
umdo {
    dialer-options {
        pool pool-name <priority priority> ;
    }
    modem-options {
        dialin (console | routable);
        init-command-string initialization-command-string;
    }
}
```

The pool name specified at the [edit interfaces umdo dialer-options pool] hierarchy level must be the same as the pool name specified at the [edit interfaces dlIn unit logical-unit-number dialer-options pool] hierarchy level.

Configure the USB modem to operate as a dial-in WAN backup interface by including the dialin statement and specifying the routable option. If the USB modem is to be used as a dial-in console, specify the console option in the dialin statement.
When the Services Router applies the modem AT commands configured in the *init-command-string* statement 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 router overrides the existing modem values that do not match. For example, if the initialization commands on the modem include S0=0 and the router’s *init-command-string* configuration includes S0=2, the Services Router applies S0=2.

- If the initialization commands on the modem do not include a command in the router’s *init-command-string* statement configuration, the router adds it. For example, if the *init-command-string* statement includes the command L2, but the modem commands do not include it, the router adds L2 to the initialization commands configured on the modem.

Include the following statements at the [edit interfaces dln] hierarchy level to support a minimum configuration for a dialer interface connected to a USB modem:

```conf
[edit interfaces dln]
encapsulation ppp;
unit logical-unit-number;
dialer-options {
  dial-string dial-string-numbers;
  pool pool-name <priority priority>;
}
ppp-options {
  chap;
  access-profile name;
  local-name name;
  passive;
}
family inet {
  mtu bytes;
  address address {
    destination address;
  }
}
```
PART 4

Monitoring and Troubleshooting Interfaces

- Monitoring Interfaces on page 335
- Troubleshooting Interfaces on page 341
CHAPTER 11

Monitoring Interfaces

- Tracing Interface Operations Overview on page 335
- Tracing Operations of an Individual Router Interface on page 335
- Tracing Operations of the Interface Process on page 336
- Monitoring a PPP Session on page 338
- Tracing Operations of the pppd Process on page 338

Tracing Interface Operations Overview

You can trace the operations of individual router interfaces and those of the interface process (dcd). For a general discussion of tracing and of the precedence of multiple tracing operations, see the Junos OS Administration Library.

For information about the operations of Virtual Router Resolution Protocol (VRRP)-enabled interfaces, see the High Availability Feature Guide.

Tracing Operations of an Individual Router Interface

To trace the operations of individual router interfaces, perform the following steps:

1. In configuration mode, go to the [edit interfaces interface-name] hierarchy level:

   [edit]
   user@host# edit interfaces interface-name

2. Configure the traceoptions option.

   [edit interfaces interface-name]
   user@host# edit traceoptions

3. Configure the tracing flag.
You can specify the following interface tracing flags:

- **all**—Trace all interface operations.
- **event**—Trace all interface events.
- **ipc**—Trace all interface interprocess communication (IPC) messages.
- **media**—Trace all interface media changes.

The interfaces `traceoptions` statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system `syslog` files.

For more information about trace operations, see "Tracing Operations of the Interface Process" on page 336.

### Tracing Operations of the Interface Process

To trace the operations of the router or switch interface process, dcd, perform the following steps:

1. In configuration mode, go to the `[edit interfaces]` hierarchy level:

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

2. Configure the `traceoptions` statement.

   ```
   [edit interfaces]
   user@host# edit traceoptions
   ```

3. Configure the `no-remote-trace` option to disable remote tracing.

   ```
   [edit interfaces traceoptions]
   user@host# set no-remote-trace
   ```

4. Configure the `file filename` option.

   ```
   [edit interfaces traceoptions]
   user@host# edit file
   ```

5. Configure the `files number` option, `match regular-expression` option, `size size` option, and `world-readable | no-world-readable` option.
Configure the tracing flag.

[edit interfaces traceoptions]
user@host# set flag flag-option

7. Configure the disable option in flag flag-option statement to disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

[edit interfaces traceoptions]
user@host# set flag flag-option disable

You can specify the following flags in the interfaces traceoptions statement:

- all—Enable all configuration logging.
- change-events—Log changes that produce configuration events.
- gres-events—Log the events related to GRES.
- resource-usage—Log the resource usage for different states.
- config-states—Log the configuration state machine changes.
- kernel—Log configuration IPC messages to kernel.
- kernel-detail—Log details of configuration messages to kernel.
- select-events—Log the events on select state machine.

By default, interface process operations are placed in the file named dcd and three 1-MB files of tracing information are maintained.

For general information about tracing, see the tracing and logging information in the Junos OS Administration Library.

Related Documentation
- Tracing Interface Operations Overview on page 335
- Tracing Operations of an Individual Router Interface on page 335
- traceoptions on page 1053
Monitoring a PPP Session

You can monitor PPP packet exchanges. When monitoring is enabled, packets exchanged during a session are logged by default to `/var/log/pppd`, or to the file specified in the `traceoptions` statement.

To monitor a PPP session:

1. In configuration mode, go to the `[edit protocols ppp]` hierarchy level.

   ```
   [edit ]
   user@host# edit protocols ppp
   ```

2. Include the `monitor-session` statement.

   ```
   [edit protocols ppp]
   user@host# monitor-session (interface-name | all);
   ```

When monitoring is configured, the operational mode commands `show ppp summary` and `show ppp interface` display a `Monitored` flag in the `Session flags` column or line.

Related Documentation

`monitor-session` on page 794

Tracing Operations of the pppd Process

You can trace the operations of the router’s pppd process.

To trace the router’s pppd process:

1. In configuration mode, go to the `[edit protocols ppp]` hierarchy level.

   ```
   [edit ]
   user@host# edit protocols ppp
   ```

2. Include the `traceoptions` statement.

   ```
   [edit protocols ppp]
   traceoptions {
     file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
     flag flag;
     level severity-level;
     no-remote-trace;
   }
   ```

   • To specify more than one tracing operation, include multiple `flag` statements.
You can specify the following flags in the `traceoptions` statement:

- **access**—Trace access code
- **address-pool**—Trace address pool code
- **all**—Trace all areas of code
- **auth**—Trace authentication code
- **chap**—Trace challenge handshake authentication protocol code
- **ci**—Trace CI code
- **config**—Trace configuration code
- **ifdb**—Trace interface database code
- **lcp**—Trace LCP state machine code
- **memory**—Trace memory management code
- **message**—Trace message processing code
- **mlppp**—Trace multilink point-to-point protocol code
- **ncp**—Trace NCP state machine code
- **pap**—Trace password authentication protocol code
- **ppp**—Trace PPP protocol processing code
- **radius**—Trace RADIUS processing code
- **redundancy**—Trace redundancy code
- **rtsock**—Trace routing socket code
- **session**—Trace session management code
- **signal**—Trace signal handling code
- **timer**—Trace timer code
- **ui**—Trace user interface code

Related Documentation: [traceoptions on page 1069](#)
CHAPTER 12

Troubleshooting Interfaces

- Configuring Interface Diagnostics Tools to Test the Physical Layer Connections on page 341
- Troubleshooting: em0 Management Interface Link is Down on page 348
- Troubleshooting: fxp0 Management Interface Link is Down on page 349
- Troubleshooting: Faulty Ethernet Physical Interface on an M Series, an MX Series, or a T Series Router on page 351
- Time Domain Reflectometry on ACX Series Routers Overview on page 359
- Diagnosing a Faulty Twisted-Pair Cable on ACX Series Routers on page 362

Configuring Interface Diagnostics Tools to Test the Physical Layer Connections

- Configuring Loopback Testing on page 341
- Configuring BERT Testing on page 343
- Starting and Stopping a BERT Test on page 347

Configuring Loopback Testing

Loopback testing allows you to verify the connectivity of a circuit. You can configure any of the following interfaces to execute a loopback test: aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, E1, E3, NxDS0, serial, SONET/SDH, T1, and T3.

The physical path of a network data circuit usually consists of segments interconnected by devices that repeat and regenerate the transmission signal. The transmit path on one device connects to the receive path on the next device. If a circuit fault occurs in the form of a line break or a signal corruption, you can isolate the problem by using a loopback test. Loopback tests allow you to isolate segments of the circuit and test them separately.

To do this, configure a line loopback on one of the routers. Instead of transmitting the signal toward the far-end device, the line loopback sends the signal back to the originating router. If the originating router receives back its own Data Link Layer packets, you have verified that the problem is beyond the originating router. Next, configure a line loopback farther away from the local router. If this originating router does not receive its own Data Link Layer packets, you can assume that the problem is on one of the segments between the local router and the remote router’s interface card. In this case, the next troubleshooting step is to configure a line loopback closer to the local router to find the source of the problem.

Copyright © 2019, Juniper Networks, Inc.
The following types of loopback testing are supported by Junos OS:

- **DCE local**—Loops packets back on the local data circuit-terminating equipment (DCE).
- **DCE remote**—Loops packets back on the remote DCE.
- **Local**—Useful for troubleshooting physical PIC errors. Configuring local loopback on an interface allows transmission of packets to the channel service unit (CSU) and then to the circuit toward the far-end device. The interface receives its own transmission, which includes data and timing information, on the local router's PIC. The data received from the CSU is ignored. To test a local loopback, issue the `show interfaces interface-name` command. If PPP keepalives transmitted on the interface are received by the PIC, the *Device Flags* field contains the output *Loop-Detected*.
- **Payload**—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A payload loopback loops data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated.
- **Remote**—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A remote loopback loops packets, including both data and timing information, back on the remote router's interface card. A router at one end of the circuit initiates a remote loopback toward its remote partner. When you configure a remote loopback, the packets received from the physical circuit and CSU are received by the interface. Those packets are then retransmitted by the PIC back toward the CSU and the circuit. This loopback tests all the intermediate transmission segments.

Table 25 on page 342 shows the loopback modes supported on the various interface types.

**Table 25: Loopback Modes by Interface Type**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Loopback Modes</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet, Fast Ethernet, Gigabit Ethernet</td>
<td>Local</td>
<td><em>Configuring Ethernet Loopback Capability</em></td>
</tr>
<tr>
<td>Circuit Emulation E1</td>
<td>Local and remote</td>
<td><em>Configuring E1 Loopback Capability</em></td>
</tr>
<tr>
<td>Circuit Emulation T1</td>
<td>Local and remote</td>
<td><em>Configuring T1 Loopback Capability</em></td>
</tr>
<tr>
<td>E1 and E3</td>
<td>Local and remote</td>
<td><em>Configuring E1 Loopback Capability and Configuring E3 Loopback Capability</em></td>
</tr>
<tr>
<td>NxDS0</td>
<td>Payload</td>
<td><em>Configuring NxDS0 IQ and IQE Interfaces, Configuring T1 and NxDS0 Interfaces, Configuring Channelized OC12/STM4 IQ and IQE Interfaces (SONET Mode), Configuring Fractional E1 IQ and IQE Interfaces, and Configuring Channelized T3 IQ Interfaces</em></td>
</tr>
<tr>
<td>Serial (V.35 and X.21)</td>
<td>Local and remote</td>
<td>&quot;Configuring Serial Loopback Capability&quot; on page 328</td>
</tr>
</tbody>
</table>
Table 25: Loopback Modes by Interface Type (continued)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Loopback Modes</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial (EIA-530)</td>
<td>DCE local, DCE remote, local, and remote</td>
<td>“Configuring Serial Loopback Capability” on page 328</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>Local and remote</td>
<td>Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External</td>
</tr>
<tr>
<td>T1 and T3</td>
<td>Local, payload, and remote</td>
<td>Configuring T1 Loopback Capability and Configuring T3 Loopback Capability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See also Configuring the T1 Remote Loopback Response</td>
</tr>
</tbody>
</table>

To configure loopback testing, include the **loopback** statement:

```
user@host# loopback mode;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name aggregated-ether-options]
- [edit interfaces interface-name ds0-options]
- [edit interfaces interface-name e1-options]
- [edit interfaces interface-name e3-options]
- [edit interfaces interface-name fastether-options]
- [edit interfaces interface-name gigether-options]
- [edit interfaces interface-name serial-options]
- [edit interfaces interface-name sonet-options]
- [edit interfaces interface-name t1-options]
- [edit interfaces interface-name t3-options]

**Configuring BERT Testing**

To configure BERT:

- Configure the duration of the test.

  ```
  user@host#bert-period seconds;
  ```

You can configure the BERT period to last from 1 through 239 seconds on some PICs and from 1 through 240 seconds on other PICs. By default, the BERT period is 10 seconds.

- Configure the error rate to monitor when the inbound pattern is received.
[edit interfaces interface-name interface-type-options]
user@host# bert-error-rate rate;

rate is the bit error rate. This can be an integer from 0 through 7, which corresponds to a bit error rate from $10^{-0}$ (1 error per bit) to $10^{-7}$ (1 error per 10 million bits).

- Configure the bit pattern to send on the transmit path.

[edit interfaces interface-name interface-type-options]
user@host# bert-algorithm algorithm;

algorithm is the pattern to send in the bit stream. For a list of supported algorithms, enter a ? after the bert-algorithm statement; for example:

[edit interfaces t1-0/0/0 t1-options]
user@host# set bert-algorithm ?

Possible completions:
- pseudo-2e11-o152 Pattern is $2^{11} -1$ (per 0.152 standard)
- pseudo-2e15-o151 Pattern is $2^{15} - 1$ (per 0.152 standard)
- pseudo-2e20-o151 Pattern is $2^{20} - 1$ (per 0.151 standard)
- pseudo-2e20-o153 Pattern is $2^{20} - 1$ (per 0.153 standard)
  ...

For specific hierarchy information, see the individual interface types.

NOTE: The four-port E1 PIC supports only the following algorithms:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pseudo-2e11-o152</td>
<td>Pattern is $2^{11} -1$ (per 0.152 standard)</td>
</tr>
<tr>
<td>pseudo-2e15-o151</td>
<td>Pattern is $2^{15} - 1$ (per 0.152 standard)</td>
</tr>
<tr>
<td>pseudo-2e20-o151</td>
<td>Pattern is $2^{20} - 1$ (per 0.151 standard)</td>
</tr>
<tr>
<td>pseudo-2e23-o151</td>
<td>Pattern is $2^{23}$ (per 0.151 standard)</td>
</tr>
</tbody>
</table>

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.
### NOTE: The 12-port T1/E1 Circuit Emulation (CE) PIC supports only the following algorithms:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-ones-repeating</td>
<td>Repeating one bits</td>
</tr>
<tr>
<td>all-zeros-repeating</td>
<td>Repeating zero bits</td>
</tr>
<tr>
<td>alternating-double-ones-zeros</td>
<td>Alternating pairs of ones and zeros</td>
</tr>
<tr>
<td>alternating-ones-zeros</td>
<td>Alternating ones and zeros</td>
</tr>
<tr>
<td>pseudo-2e11-o152</td>
<td>Pattern is $2^{11} - 1$ (per O.152 standard)</td>
</tr>
<tr>
<td>pseudo-2e15-o151</td>
<td>Pattern is $2^{15} - 1$ (per O.151 standard)</td>
</tr>
<tr>
<td>pseudo-2e20-o151</td>
<td>Pattern is $2^{20} - 1$ (per O.151 standard)</td>
</tr>
<tr>
<td>pseudo-2e7</td>
<td>Pattern is $2^7 - 1$</td>
</tr>
<tr>
<td>pseudo-2e9-o153</td>
<td>Pattern is $2^9 - 1$ (per O.153 standard)</td>
</tr>
<tr>
<td>repeating-1-in-4</td>
<td>1 bit in 4 is set</td>
</tr>
<tr>
<td>repeating-1-in-8</td>
<td>1 bit in 8 is set</td>
</tr>
<tr>
<td>repeating-3-in-24</td>
<td>3 bits in 24 are set</td>
</tr>
</tbody>
</table>

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

### NOTE: The IQE PICs support only the following algorithms:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-ones-repeating</td>
<td>Repeating one bits</td>
</tr>
<tr>
<td>all-zeros-repeating</td>
<td>Repeating zero bits</td>
</tr>
<tr>
<td>alternating-double-ones-zeros</td>
<td>Alternating pairs of ones and zeros</td>
</tr>
<tr>
<td>alternating-ones-zeros</td>
<td>Alternating ones and zeros</td>
</tr>
<tr>
<td>pseudo-2e9-o153</td>
<td>Pattern is $2^9 - 1$ (per O.153 (511 type) standard)</td>
</tr>
<tr>
<td>pseudo-2e11-o152</td>
<td>Pattern is $2^{11} - 1$ (per O.152 and O.153 (2047 type) standards)</td>
</tr>
<tr>
<td>pseudo-2e15-o151</td>
<td>Pattern is $2^{15} - 1$ (per O.151 standard)</td>
</tr>
<tr>
<td>pseudo-2e20-o151</td>
<td>Pattern is $2^{20} - 1$ (per O.151 standard)</td>
</tr>
<tr>
<td>pseudo-2e20-o153</td>
<td>Pattern is $2^{20} - 1$ (per O.153 standard)</td>
</tr>
<tr>
<td>pseudo-2e23-o151</td>
<td>Pattern is $2^{23} - 1$ (per O.151 standard)</td>
</tr>
<tr>
<td>repeating-1-in-4</td>
<td>1 bit in 4 is set</td>
</tr>
<tr>
<td>repeating-1-in-8</td>
<td>1 bit in 8 is set</td>
</tr>
<tr>
<td>repeating-3-in-24</td>
<td>3 bits in 24 are set</td>
</tr>
</tbody>
</table>

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.
NOTE: BERT is supported on the PDH interfaces of the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP and the DS3/E3 MIC. The following BERT algorithms are supported:

- all-ones-repeating
- all-zeros-repeating
- alternating-double-ones-zeros
- alternating-ones-zeros
- repeating-1-in-4
- repeating-1-in-8
- repeating-3-in-24
- pseudo-2e9-o153
- pseudo-2e11-o152
- pseudo-2e15-o151
- pseudo-2e20-o151
- pseudo-2e20-o153
- pseudo-2e23-o151

Repeating one bits
Repeating zero bits
Alternating pairs of ones and zeros
Alternating ones and zeros
1 bit in 4 is set
1 bit in 8 is set
3 bits in 24 are set
Pattern is $2^9 - 1$ (per 0.153 standard)
Pattern is $2^{11} - 1$ (per 0.152 standard)
Pattern is $2^{15} - 1$ (per 0.151 standard)
Pattern is $2^{20} - 1$ (per 0.151 standard)
Pattern is $2^{23}$ (per 0.151 standard)

Table 26 on page 346 shows the BERT capabilities for various interface types.

Table 26: BERT Capabilities by Interface Type

<table>
<thead>
<tr>
<th>Interface</th>
<th>T1 BERT</th>
<th>T3 BERT</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-port T1/E1 Circuit Emulation</td>
<td>Yes (ports 0–11)</td>
<td>—</td>
<td>• Limited algorithms</td>
</tr>
<tr>
<td>4-port Channelized OC3/STM1 Circuit Emulation</td>
<td>Yes (port 0–3)</td>
<td>—</td>
<td>• Limited algorithms</td>
</tr>
<tr>
<td>E1 or T1</td>
<td>Yes (port 0–3)</td>
<td>Yes (port 0–3)</td>
<td>• Single port at a time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Limited algorithms</td>
</tr>
<tr>
<td>E3 or T3</td>
<td>Yes (port 0–3)</td>
<td>Yes (port 0–3)</td>
<td>• Single port at a time</td>
</tr>
<tr>
<td>Channelized OC12</td>
<td>—</td>
<td>Yes (channel 0–11)</td>
<td>• Single channel at a time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Limited algorithms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No bit count</td>
</tr>
<tr>
<td>Channelized STM1</td>
<td>Yes (channel 0–62)</td>
<td>—</td>
<td>• Multiple channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Only one algorithm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No error insert</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No bit count</td>
</tr>
<tr>
<td>Channelized T3 and Multichannel T3</td>
<td>Yes (channel 0–27)</td>
<td>Yes (port 0–3 on channel 0)</td>
<td>• Multiple ports and channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Limited algorithms for T1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No error insert for T1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• No bit count for T1</td>
</tr>
</tbody>
</table>
These limitations do not apply to channelized IQ interfaces. For information about BERT capabilities on channelized IQ interfaces, see Channelized IQ and IQE Interfaces Properties.

Starting and Stopping a BERT Test

Before you can start the BERT test, you must disable the interface. To do this, include the disable statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
disable;
```

After you configure the BERT properties and commit the configuration, begin the test by issuing the `test interface interface-name interface-type-bert-start` operational mode command:

```
user@host> test interface interface-name interface-type-bert-start
```

The test runs for the duration you specify with the `bert-period` statement. If you want to terminate the test sooner, issue the `test interface interface-name interface-type-bert-stop` command:

```
user@host> test interface interface-name interface-type-bert-stop
```

For example:

```
user@host> test interface t3-1/2/0 t3-bert-start
user@host> test interface t3-1/2/0 t3-bert-stop
```

To view the results of the BERT test, issue the `show interfaces extensive | find BERT` command:

```
user@host> show interfaces interface-name extensive | find BERT
```

For more information about running and evaluating the results of the BERT procedure, see the CLI Explorer.

**NOTE:** To exchange BERT patterns between a local router and a remote router, include the loopback remote statement in the interface configuration at the remote end of the link. From the local router, issue the test interface command.

**Related Documentation**

- `show interfaces diagnostics optics (Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, 100-Gigabit Ethernet, and Virtual Chassis Port)`
Troubleshooting: em0 Management Interface Link is Down

Problem  Description: Ethernet Link Down alarm is raised when you run the show chassis alarm operational mode command on a T640 router, a T1600 router, T4000 router, or a TX Matrix Plus router.

Diagnosis  Perform the following tests to check if the em0 management interface is down on the master Routing Engine or the backup Routing Engine:

1. Run the show chassis alarms command.

```
show chassis alarms
```

```
user@host0> show chassis alarms
1 alarms currently active
Alarm time  Class Description
2011-10-19 11:13:02  MYT Major Host 1 em0 : Ethernet Link Down
```

Is the alarm Ethernet Link Down displayed against the em0 interface of the master Routing Engine (Host 0)?

- **Yes:** Contact JTAC for further assistance.
- **No:** Continue to the next diagnostic test.

2. Run the show interfaces em0 and the show interfaces em0 terse operational mode commands.

```
show interfaces em0
```

```
user@host> show interfaces em0
Physical interface: em0, Enabled, Physical link is Up
Interface index: 1, SNMP ifIndex: 1
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
...
```

```
show interfaces em0 terse
```

```
user@host> show interfaces em0 terse
Interface Admin Link Proto Local Remote
dem0 up up inet 10.100.100.1/30
```

Is the em0 interface on the master Routing Engine **up**?

- **Yes:** Continue to resolution.
Resolution  

To Resolve This Issue

From the aforementioned diagnosis, we ascertain that the chassis alarm has been raised for the em0 management interface in the backup Routing Engine (Host 1) and not for the master Routing Engine (Host 0).

Implement one of the following solutions on the backup Routing Engine to resolve this issue:

• Disable the em0 interface in the backup Routing Engine:
  1. In configuration mode, go to the [edit groups re1] hierarchy level.

     user@host1# edit groups re1

  2. Disable the em0 interface.

     [edit groups re1]
     user@host1# set interfaces em0 disable

• Ignore the alarm:
  1. In configuration mode, go to the [edit chassis] hierarchy level.

     user@host1# edit chassis

  2. Ignore the Ethernet link down alarm on the management interface by setting the management-ethernet link-down alarm option to ignore.

     [edit chassis]
     user@host1# set alarm management-ethernet link-down ignore

Related Documentation

• Supported Routing Engines by Router
• show chassis alarms

Troubleshooting: fxp0 Management Interface Link is Down

Problem  Description: Ethernet Link Down alarm is raised when you run the show chassis alarm operational mode command on an M Series router, an MX Series router, a T320 router, a T640 router, a T1600 router, or on a TX Matrix router.
**Diagnosis**

Perform the following tests to check if the fxp0 interface is down on the master Routing Engine or the backup Routing Engine:

1. Run the `show chassis alarms` command.

   ```
   user@host0> show chassis alarms
   1 alarms currently active
   Alarm time Class Description
   2011-10-19 11:13:02 MYT Major Host 1 fxp0 : Ethernet Link Down
   ```

   Is the alarm *Ethernet Link Down* displayed against the fxp0 interface of the master Routing Engine (Host 0)?
   - Yes: Contact JTAC for further assistance.
   - No: Continue to the next diagnostic test.

2. Run the `show interfaces fxp0` and the `show interfaces fxp0 terse` operational mode commands.

   ```
   user@host> show interfaces fxp0
   Physical interface: fxp0, Enabled, Physical link is Up
   Interface index: 1, SNMP ifIndex: 1
   Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
   Device flags : Present Running
   Interface flags: SNMP-Traps
   ```

   ```
   user@host> show interfaces fxp0 terse
   Interface Admin Link Proto Local Remote
   fxp0 up up
   fxp0.0 up up inet 10.100.100.1/30
   ```

   Is the fxp0 interface on the master Routing Engine *up*?
   - Yes: Continue to resolution.
   - No: Contact JTAC for further assistance

**Resolution**

*To Resolve This Issue*

From the diagnosis, we ascertain that the chassis alarm has been raised for the fxp0 management interface in the backup Routing Engine (Host 1) and not for the master Routing Engine (Host 0).
Implement one of the following solutions on the backup Routing Engine to avoid this issue:

- Disable the fxp0 interface in the backup Routing Engine:
  1. In configuration mode, go to the [edit groups re1] hierarchy level.

     user@host1# edit groups re1

  2. Disable the fxp0 interface.

     [edit groups re1]
     user@host1# set interfaces fxp0 disable

- Ignore the alarm:
  1. In configuration mode, go to the [edit chassis] hierarchy level.

     user@host1# edit chassis

  2. Ignore the Ethernet link down alarm on the management interface by setting the management-ethernet link-down alarm option to ignore.

     [edit chassis]
     user@host1# set alarm management-ethernet link-down ignore

**Related Documentation**
- Supported Routing Engines by Router
- show chassis alarms

**Troubleshooting: Faulty Ethernet Physical Interface on an M Series, an MX Series, or a T Series Router**

You can follow the basic troubleshooting checklist as explained in the following topics from one through five to troubleshoot an Ethernet physical interface on an M Series, MX Series, or a T Series router.

1. Checking the Cable Connection on page 352
2. Checking the Physical Link Status of the Interface on page 353
3. Checking the Interface Statistics in Detail on page 354
4. Performing the Loopback Diagnostic Test on page 356
5. Checking Other Possibilities on page 358
6. To Enable a Physical Interface on page 359
Checking the Cable Connection

**Problem Description:** Packets are not received or transmitted over the Ethernet physical interface.

**Diagnosis**

1. Is the correct cable connected to the correct port?
   - Yes: Continue to “Checking the Physical Link Status of the Interface” on page 353.
   - No: See “Resolving Cabling Issue” on page 352.

**Resolution**

*Resolving Cabling Issue*

Perform one or more of the following steps to resolve the cabling issue:

1. Connect the cable properly on the local and remote ends without any loose connections.

2. Swap the Ethernet cable for a known good cable if the existing cable is damaged.

3. Connect a single-mode fiber cable to a single-mode interface only and a multimode fiber cable to a multimode interface only. To check fiber optic cable integrity, see “Checking Fiber Optic Cable Integrity” on page 352.

4. Connect the correct small form-factor pluggable transceiver (SFP) on both sides of the cable.

*Checking Fiber Optic Cable Integrity*

To check the integrity of fiber optic cable with an external cable diagnostic testing tool:

**NOTE:** A single-mode fiber cable must be connected to a single-mode interface and a multi-mode fiber cable must be connected to a multi-mode interface.

1. Measure the received light level at the receiver (RX) port to see whether the received light level is within the receiver specification of the Ethernet interface.

2. Measure transmitted light level at the transmitter (TX) port to see whether the transmitted light level is within the transmitter specification of the Ethernet interface.
Checking the Physical Link Status of the Interface

Problem Description: Unable to transmit and receive packets on the Ethernet interface even though the cable connection is correct.

Solution
To display the physical link status of the interface, run the `show interface interface-name media` operational mode command. For example, on the ge-5/0/1 interface.

```
user@host> show interfaces ge-5/0/1 media
Physical interface: ge-5/0/1, Enabled, Physical link is Up
    Interface index: 317, SNMP ifIndex: 1602
    Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, BPDU Error: None,
    MAC-REWRITE Error: None, Loopback: Disabled,
    Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
    Remote fault: Online, Speed-negotiation: Disabled, Auto-MDI: Enabled
    Device flags : Present Running
    Interface flags: SNMP-Traps Internal: 0x4000
    Link flags   : None
    CoS queues   : 8 supported, 8 maximum usable queues
    Current address: 2c:6b:f5:4c:26:73, Hardware address: 2c:6b:f5:4c:26:73
    Last flapped : 2012-11-30 01:25:37 UTC (03:46:55 ago)
    Input rate   : 880 bps (1 pps)
    Output rate  : 312 bps (0 pps)
    Active alarms: None
    Active defects: None
    MAC statistics:
    Input bytes: 901296, Input packets: 9799, Output bytes: 976587, Output packets: 10451
    Filter statistics:
    Filtered packets: 68, Padded packets: 0, Output packet errors: 0
    Autonegotiation information:
    Negotiation status: Complete
    Link partner:
    Link mode: Full-duplex, Flow control: Symmetric/Asymmetric, Remote fault: OK
    Local resolution:
    Flow control: Symmetric, Remote fault: Link OK
    Interface transmit statistics: Disabled
```

For information about `show interfaces interface-name media`, see `show interfaces`.

Diagnosis
1. Are there any connectivity problems such as input errors and packet loss even though the Enabled field displays Physical link is Up status and the Active alarms and Active defect field displays None?
   - Yes: Go to “Checking the Interface Statistics in Detail” on page 354.
   - No: Continue to the next diagnostic test.
2. Does the Enabled field display Physical link is Down status and the Active alarms and Active defect field display Link?

- Yes: The interface is either not connected correctly or is not receiving a valid signal. Go to “Resolving Cabling Issue” on page 352.
- No: Continue.

Checking the Interface Statistics in Detail

**Problem Description:** The physical interface is not working even though the Enabled field displays Physical link is Up status and the Active alarms and Active defect field displays None.

**Solution** To display the interface statistics in detail, run the show interface interface-name extensive operational command. For example, on ge-5/0/1 interface.

```
user@host> show interfaces ge-5/0/1 extensive
Physical interface: ge-5/0/1, Enabled, Physical link is Up
   Interface index: 317, SNMP ifIndex: 1602, Generation: 322
   Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, BPDU Error: None,
   MAC-REWRITE Error: None, Loopback: Disabled,
   Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
   Remote fault: Online, Speed-negotiation: Disabled,
   Auto-MDIX: Enabled
   Device flags   : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Link flags     : None
   CoS queues     : 8 supported, 8 maximum usable queues
   Hold-times     : Up 0 ms, Down 0 ms
   Current address: 2c:6b:f5:4c:26:73, Hardware address: 2c:6b:f5:4c:26:73
   Last flapped   : 2012-11-30 01:25:37 UTC (04:38:32 ago)
   Statistics last cleared: Never
   Traffic statistics:
   Input  bytes  :               806283                    0 bps
   Output bytes :              1153215                  424 bps
   Input  packets:                10818                    0 pps
   Output packets:                11536                    0 pps
   IPv6 transit statistics:
    Input  bytes :                    0
    Output bytes :                    0
    Input  packets:                    0
    Output packets:                    0
   Label-switched interface (LSI) traffic statistics:
    Input  bytes :                    0
    Input  packets:                    0
   Dropped traffic statistics due to STP State:
    Input  bytes :                    0
    Output bytes :                    0
    Input  packets:                    0
    Output packets:                    0
   Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 233060,
    L3 incompletes: 0, L2 channel errors: 0,
    L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
```
Carrier transitions: 11, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use

Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 3216 3216 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 8320 8320 0

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control

Active alarms: None
Active defects: None

MAC statistics: Receive Transmit
Total octets 1007655 1082219
Total packets 10886 11536
Unicast packets 4350 4184
Broadcast packets 32 77
Multicast packets 6504 7275
CRC/Align errors 0 0
FIFO errors 0 0
MAC control frames 0 0
MAC pause frames 0 0
Oversized frames 0 0
Jabber frames 0 0
Fragment frames 0 0
VLAN tagged frames 0 0
Code violations 0 0

Filter statistics:
Input packet count 10886
Input packet rejects 68
Input DA rejects 68
Input SA rejects 0
Output packet count 11536
Output packet pad count 0
Output packet error count 0

CAM destination filters: 0, CAM source filters: 0

Autonegotiation information:
Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: Symmetric/Asymmetric, Remote fault: OK

Local resolution:
  Flow control: Symmetric, Remote fault: Link OK

Packet Forwarding Engine configuration:
  Destination slot: 5

CoS information:
  Direction: Output
  CoS transmit queue Bandwidth Buffer Priority Limit

Copyright © 2019, Juniper Networks, Inc.
For information about `show interfaces interface-name detail`, see `show interfaces`.

**Diagnosis**

1. Does the **Policed discards**, **L2 channel errors**, **Input DA rejects**, or the **Input SA rejects** field display any errors?

   For information about the errors, see `show interfaces`.
   - Yes: Resolve the errors as needed. Resolving these errors is beyond the scope of this topic.
   - No: Continue with “Performing the Loopback Diagnostic Test” on page 356.

**Performing the Loopback Diagnostic Test**

**Problem Description:** The interface cable is connected correctly and there are no alarms or errors associated with the Ethernet physical interface yet the interface is not working.

**Solution**

To check whether the Ethernet port or PIC is faulty, you must perform the internal loopback test and hardware loopback test.

To perform a internal loopback diagnostic test on an Ethernet interface, for example on ge-5/0/1 interface:

1. In configuration mode, go to the `[edit interfaces ge-5/0/1]` hierarchy level.

   ```plaintext
   [edit]
   user@host# edit interface ge-5/0/1
   ```

2. Set the `gigether-options` option as loopback, commit the configuration and quit configuration mode.

   ```plaintext
   [edit interfaces ge-5/0/1]
   user@host# set gigether-options loopback
   user@host# commit
   user@host# quit
   ```

3. In operational mode, execute the `show interfaces ge-5/0/1 media` command.
user@host> show interfaces ge-5/0/1 media
Physical interface: ge-5/0/1, Enabled, Physical link is Up
    Interface index: 317, SNMP ifIndex: 1602
    Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, BPDU Error: None,
    MAC-REWRITE Error: None, Loopback: Enabled,
    Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
    Remote fault: Online, Speed-negotiation: Disabled,
    Auto-MDIX: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Current address: 2c:6b:f5:4c:26:73, Hardware address: 2c:6b:f5:4c:26:73
Last flapped   : 2012-11-30 01:25:37 UTC (03:46:55 ago)
Input rate     : 880 bps (1 pps)
Output rate    : 312 bps (0 pps)
Active alarms  : None
Active defects : None
MAC statistics:
    Input bytes: 901296, Input packets: 9799, Output bytes: 976587, Output
    packets: 10451
Filter statistics:
    Filtered packets: 68, Padded packets: 0, Output packet errors: 0
Autonegotiation information:
    Negotiation status: Complete
Link partner:
    Link mode: Full-duplex, Flow control: Symmetric/Asymmetric, Remote
    fault: OK
    Local resolution:
        Flow control: Symmetric, Remote fault: Link OK
Interface transmit statistics: Disabled

NOTE: Delete the loopback statement after completing your diagnosis.

Execute one of the following steps for a hardware loopback diagnostic test as needed:

- For an Ethernet PIC with a fiber optic interface—Physically loop the T_x and R_x port
  and check the status of the physical link with the show interfaces interface-name media
  operational mode command.

- For an Ethernet PIC with an RJ-45 Ethernet interface—Build a loopback plug by crossing
  pin 1 (T_x +) to pin 3 (R_x +) together and pin 2 (T_x -) and pin 6 (R_x -) together and check
  the status of the physical link with the show interfaces interface-name media operational
  mode command.
NOTE: For information about loopback testing, see Performing Loopback Testing for Fast Ethernet and Gigabit Ethernet Interfaces.

Diagnosis

1. Does the Enabled field display Physical link is Up status and the Active alarms and Active defect field display None when you perform the loopback test?
   - Yes: Go to the “Checking Other Possibilities” on page 358 section.
   - No: Continue to the next diagnostic test.

2. When the Ethernet interface is connected to a remote Ethernet device over multiple patch panels, check to see whether the connection can be looped back at the different patch panels so you can conduct a loopback diagnostic test. Is the loopback diagnostic test successful?
   - Yes: Go to the “Checking Other Possibilities” on page 358 section.
   - No: Contact JTAC for further assistance.

Checking Other Possibilities

Problem Description: Loopback diagnostic test is successful but unable to transmit and receive packets on the Ethernet interface.

Solution

Use the following commands as needed to troubleshoot an Ethernet interface, for example, an ge-5/0/1 interface:

- Run the show interfaces interface-name terse operational command to check if the physical interface and logical interfaces are administratively disabled. For example, on ge-5/0/1 interface.

```
user@host> show interfaces ge-5/0/1 terse

Interface           Admin Link Proto    Local                 Remote
ge-5/0/1             up      up    inet     20.1.1.2/24
ge-5/0/1.0            up      up   inet        0.0.0.0
ge-5/0/1.1           up      up   inet        0.0.0.0
```

Diagnosis

1. Does the physical interface and its corresponding logical interfaces display down in the output of the show interfaces interface-name terse operational mode command?
   - Yes: Enable the interfaces as shown in “To Enable a Physical Interface” on page 359.
   - No: Continue to the next diagnostic test.
2. Are the speed, duplex, and auto-negotiation fields in the output of `show interfaces interface-name extensive` operational mode command correctly set for the interface?

   **NOTE:** Check if the associated Flexible PIC Concentrator (FPC), Modular Port Concentrator (MPC), or Dense Port Concentrator (DPC) and its Modular Interface Card (MIC) or PIC with its 10-gigabit small form-factor pluggable transceiver (XFP) or SFP supports speed and auto-negotiation settings.

   - Yes: Check Monitoring Fast Ethernet and Gigabit Ethernet Interfaces for more troubleshooting tips.
   - No: Contact JTAC for further assistance.

**To Enable a Physical Interface**

To enable a physical interface:

1. In configuration mode, go to the `[edit interfaces]` hierarchy level.

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

2. Check if the interface is administratively disabled by executing the `show` command on the interface. For example on ge-5/0/1 interface.

   ```
   user@host# show ge-5/0/1
   disable;
   ```

3. Enable the interface and commit.

   ```
   [edit interfaces
   user@host# delete interface-name disable
   user@host# commit
   ```

   **See Also**  
   - `show interfaces` on page 1161

**Time Domain Reflectometry on ACX Series Routers Overview**

Time Domain Reflectometry (TDR) is a technology used for diagnosing copper cable states. This technique can be used to determine if cabling is at fault when you cannot establish a link. TDR detects the defects by sending a signal through a cable, and reflecting it from the end of the cable. Open circuits, short circuits, sharp bends and other defects
in the cable, reflects the signal back, at different amplitudes, depending on the severity of the defect.

Several factors that result in degraded or low-quality cable plants can cause packet loss, suboptimal connection speed, reduced network efficiency, and complete connection failures. These types of problems can occur because of poor cable construction, identification of pair twists, loose connectors, poor contacts between the points, and stretched or broken pairs of cables. Broadcom transceivers enable you to analyze the condition of the cable plant or topology and identify any problems that have occurred. This functionality is effectively used in the following scenarios:

- Troubleshooting during initial network equipment installation.
- Discovery of failures when network problems occur.
- Maintenance of optimally functioning cable plants.
- Fault determination during the testing of network equipment in production cable networks.

TDR supports the following capabilities for examination of cable faults on ACX Series routers:

- Cable status pair (open or short)—When the router operates in Gigabit Ethernet mode, all the four pairs (8 wires) are used. Only Pair-A and Pair-B are required to operate in 10/100BASE-T Ethernet mode. If either of these required pairs is open or short-circuited, the transceiver reports the following faults:
  - Any open wire
  - Wires of a particular pair that are shorted
- Distance to fault per pair—Distance at which an open or a short-circuit is detected in meters. This measurement is also termed as cable length. The transceiver reports the following faults:
  - Cable length when the cable status is normal
  - Distance to fault when the cable status is not normal
- Pair Swap—Swapping of twisted-pairs in straight-through and cross-over cable plants are detected.
- Polarity Swap—Each cable pair carries a differential signal from one end to the other end of the cable. Each wire within the pair is assigned a polarity. The wires in a pair are normally connected in a one-to-one form. This connection enables the transmitter at one end to be connected to the receiver at the other end with same polarity. Sometimes, the wiring within the pair is also swapped. This type of connection is called polarity swap. Broadcom transceivers can detect such swapping and automatically adjust the connection to enable the links to operate normally. However, the transceiver reports polarity swaps that it detects in the cable plant.

On 4-port Gigabit Ethernet and 8-port Gigabit Ethernet MICs with copper SFP transceivers (using BCM54880) and 4-port Gigabit Ethernet, 6-port Gigabit Ethernet, and 8-port Gigabit Ethernet MICs with copper and optical SFP transceivers (using BCM54640E
PHY), only 10BASE-T pair polarity is supported. 100BASE-T and 1000BASE-T polarities are not supported.

When the Gigabit Ethernet link cannot be established (for example, if only two pairs are present that are fully functional), TDR in the physical layer (PHY) brings down the link to a 100 MB link, which is called a downshift in the link. The physical layer might require 10-20 seconds for the link to come up if a downgrade in wire speed occurs because it attempts to connect at 1000 MB five times before it falls back to 100BASE-TX.

TDR diagnostics is supported only on copper interfaces and not on fiber interfaces.

Keep the following points in mind when you configure TDR:

- If you connect a port undergoing a TDR test to a Gigabit Ethernet interface that is enabled to automatically detect MDI (Media Dependent Interface) and MDIX (Media Dependent Interface with Crossover) port connections, the TDR result might be invalid.
- If you connect a port undergoing a TDR test to a 100BASE-T copper interface, the unused pairs are reported as faulty because the remote end does not terminate these pairs.
- You must not modify the port configuration while the TDR test is running.
- Because of cable characteristics, you need to run the TDR test multiple times to get accurate results.
- Do not change the port status (such as removing the cable at the near or far end) because such a change can result in inaccurate statistics in the results.
- While measuring the cable length or distance to fault (per pair), sometimes, a few cable length inconsistencies might be observed during a TDR test. Broadcom transceivers have the following cable length limitations:
  - For a properly-terminated good cable, the accuracy of the cable length reported is plus or minus 10 meters.
  - If a pair is open or short-circuited, the far-end termination does not affect the computed result for that pair.
  - The accuracy of the measured cable length, when open and short-circuit conditions are detected, is plus or minus 5 meters.
  - The accuracy of a good pair, when one or more pairs are open or short-circuited, is plus or minus 10 meters.
- Polarity swap detection is supported only in 10BASE-T mode.
- The TDR test does not impact the traffic if the interface operates at 10-Gigabit Ethernet per second of bandwidth, which is the default configuration. However, if the speed of the interface is configured to be other than 10-Gigabit Ethernet, running the TDR test affects the traffic.

TDR diagnostics might bring the link down and initialize the physical layer (PHY) with default configuration to perform its operation.

When the TDR validation test is completed, the PHY layer resumes operation in the same manner as before the cable diagnostics test was performed. However, link flaps
might be momentarily observed. We recommend that you run the TDR test at a speed of 1 gigabit per second, which is the default configuration, to obtain more accurate results.

TDR is supported on the following interfaces on ACX Series routers:

- On ACX1000 routers, 4 RJ45 (Cu) ports or 8-port Gigabit Ethernet MICs with small form-factor pluggable (SFP) transceivers and RJ45 connectors.
- On ACX1100 routers, 4-port or 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX2000 routers, 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX2100 and ACX22000 routers, 4-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX4000 routers, 4-port, 6-port, or 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.

You must select the media type as copper for the 1-Gigabit Ethernet interfaces. To specify the media type, include the `media-type` statement with the `copper` option at the `[edit interfaces interface-name]` hierarchy level. Media type selection is applicable to ports only in slot 2. When media-type is not set, the port accepts either type of connection. The media type is fiber if a transceiver is installed in the SFP connection. If no transceiver is installed, the media type is copper. The COMBO ports (combination ports) on ACX routers support both the copper and fiber-optic media types. On such ports or interfaces, you must configure the media type as copper to run the TDR test.

You can run the TDR test from operational mode and view the success or failure results of the test. To start a test on a specific interface, issue the `request diagnostics tdr start interface interface-name` command. To stop the TDR test currently in progress on the specified interface, issue the `request diagnostics tdr abort interface interface-name` command. To display the test results for all copper interfaces, enter the `show diagnostics tdr` command. To display the test results for a particular interface, enter the `show diagnostics tdr interface interface-name` command.

**Related Documentation**

- Diagnosing a Faulty Twisted-Pair Cable on ACX Series Routers on page 362

**Diagnosing a Faulty Twisted-Pair Cable on ACX Series Routers**

**Problem**

**Description:** A 10/100BASE-T Ethernet interface has connectivity problems that you suspect might be caused by a faulty cable.

**Solution**

Use the time domain reflectometry (TDR) test to determine whether a twisted-pair Ethernet cable is faulty.

The TDR test:
- Detects and reports faults for each twisted pair in an Ethernet cable. Faults detected include open circuits, short circuits, and impedance mismatches.
- Reports the distance to fault to within 1 meter.
- Detects and reports pair swaps, pair polarity reversals, and excessive pair skew.

The TDR test is supported on the following ACX routers and interfaces:

- On ACX1000 routers, 4 RJ45 (Cu) ports or 8-port Gigabit Ethernet MICs with small form-factor pluggable (SFP) transceivers and RJ45 connectors.
- On ACX1100 routers, 4-port or 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX2000 routers, 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX2100 and ACX2200 routers, 4-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.
- On ACX4000 routers, 4-port, 6-port, or 8-port Gigabit Ethernet MICs with SFP transceivers and RJ45 connectors.

**NOTE:** We recommend running the TDR test on an interface when there is no traffic on the interface.

TDR diagnostics are applicable for copper ports only and not for optical fiber ports.

To diagnose a cable problem by running the TDR test:

1. Run the *request diagnostics tdr* command.

```
user@host> request diagnostics tdr start interface ge-0/0/10
Interface TDR detail:
Test status                     : Test successfully executed  ge-0/0/10
```

2. View the results of the TDR test with the *show diagnostics tdr* command.

```
user@host> show diagnostics tdr interface ge-0/0/10
Interface TDR detail:
Interface name                  : ge-0/0/10
Test status                     : Passed
Link status                     : Down
MDI pair                        : 1-2
   Cable status                  : Normal
   Distance fault                : 0 Meters
   Polarity swap                 : N/A
   Skew time                     : N/A
MDI pair                        : 3-6
```
Cable status                  : Normal
Distance fault                : 0 Meters
Polarity swap                 : N/A
Skew time                     : N/A
MDI pair                        : 4-5
Cable status                  : Open
Distance fault                : 1 Meters
Polarity swap                 : N/A
Skew time                     : N/A
MDI pair                        : 7-8
Cable status                  : Normal
Distance fault                : 0 Meters
Polarity swap                 : N/A
Skew time                     : N/A
Channel pair                    : 1
Pair swap                     : N/A
Channel pair                    : 2
Pair swap                     : N/A
Downshift                       : N/A

3. Examine the **Cable status** field for the four MDI pairs to determine if the cable has a fault. In the preceding example, the twisted pair on pins 4 and 5 is broken or cut at approximately one meter from the **ge-0/0/10** port connection.

**NOTE:** The **Test Status** field indicates the status of the TDR test, not the cable. The value *Passed* means the test completed—it does not mean that the cable has no faults.

The following is additional information about the TDR test:

- The TDR test can take some seconds to complete. If the test is still running when you execute the `show diagnostics tdr` command, the **Test status** field displays *Started*. For example:

  ```
  user@host> show diagnostics tdr interface ge-0/0/22
  Interface TDR detail:
  Interface name : ge-0/0/22
  Test status    : Started
  ```

- You can terminate a running TDR test before it completes by using the `request diagnostics tdr abort interface interface-name` command. The test terminates with no results, and the results from any previous test are cleared.

- You can display summary information about the last TDR test results for all interfaces on the router that support the TDR test by not specifying an interface name with the `show diagnostics tdr` command. For example:

  ```
  user@host> show diagnostics tdr
  Interface   Test status    Link status  Cable status  Max distance fault
  ```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>State</th>
<th>Check</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Passed</td>
<td>Down</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Passed</td>
<td>Down</td>
<td>Fault</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Passed</td>
<td>Down</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Time Domain Reflectometry on ACX Series Routers Overview on page 359
- `request diagnostics tdr`
- `show diagnostics tdr`
PART 5

Configuration Statements and Operational Commands

- Configuration Statements on page 369
- Interface Operational Commands on page 1151
- ANCP Operational Commands on page 1669
- BFD Operational Commands on page 1713
- BGP Operational Commands on page 1729
- ES-IS Operational Commands on page 1779
- IP Multicast Operational Commands on page 1789
- IPv6 Operational Commands on page 2035
- IS-IS Operational Commands on page 2045
- LLDP Operational Commands on page 2111
- MVRP Operational Commands on page 2135
- OSPF Operational Commands on page 2153
- Protocol-Independent Routing Operational Commands on page 2239
- RIP Operational Commands on page 2513
- RIPng Operational Commands on page 2525
- Firewall Filter Operational Commands on page 2535
- Layer 2 Bridging and Switching Operational Commands on page 2557
- VPN Operational Commands on page 2589
CHAPTER 13

Configuration Statements

- 802.3ad on page 388
- accept on page 389
- accept-source-mac on page 391
- access-concentrator on page 393
- access-profile on page 394
- accounting on page 395
- accounting-profile on page 396
- acfc on page 397
- acknowledge-retries on page 398
- acknowledge-timer on page 399
- action (OAM) on page 400
- action (Policer) on page 400
- action-profile (Applying to CFM) on page 401
- action-profile (Defining for CFM) on page 402
- action-profile on page 403
- action-red-differential-delay on page 404
- activation-delay on page 405
- activation-priority on page 406
- address on page 407
- advertise-interval on page 409
- age on page 410
- agent-specifier on page 411
- aggregate (Gigabit Ethernet CoS Policer) on page 412
- aggregate (Hierarchical Policer) on page 413
- aggregate (SONET/SDH) on page 414
- aggregate-ports on page 414
- aggregated-ether-options on page 415
- aggregated-sonet-options on page 416
• alarm (optics-options) on page 417
• alias (Interfaces) on page 418
• allow-any-vci on page 419
• allow-fragmentation on page 420
• allow-remote-loopback on page 421
• annex on page 421
• apply-action-profile on page 422
• aps on page 423
• arp (Interfaces) on page 424
• asynchronous-notification on page 428
• atm-encapsulation on page 429
• atm-options on page 430
• atm-scheduler-map on page 431
• authentication on page 432
• authentication-key on page 433
• authentication-profile-name on page 433
• authenticator on page 434
• auto-configure on page 435
• auto-discovery on page 436
• auto-negotiation on page 437
• backup-destination on page 439
• backup-interface on page 439
• backup-options on page 440
• bandwidth (Interfaces) on page 441
• bandwidth-limit (Hierarchical Policer) on page 442
• bandwidth-limit (Policer for Gigabit Ethernet Interfaces) on page 443
• bearer-bandwidth-limit on page 444
• bert-algorithm on page 445
• bert-error-rate on page 447
• bert-period on page 449
• bridge-domain on page 450
• broadcast on page 451
• buildout (E3 or T3 over ATM Interfaces) on page 452
• buildout (T1 Interfaces) on page 453
• bundle on page 454
• burst-size-limit (Hierarchical Policer) on page 455
• burst-size-limit (Policer for Gigabit Ethernet Interfaces) on page 456
- byte-encoding on page 457
- bytes on page 458
- calculation-weight on page 459
- callback on page 460
- callback-wait-period on page 461
- caller on page 462
- calling-number on page 463
- cbit-parity on page 464
- cbr on page 465
- cell-bundle-size on page 466
- chap on page 467
- circuit-type on page 468
- cisco-interoperability on page 468
- classifier on page 469
- clear-dont-fragment-bit on page 470
- clock-rate on page 471
- clocking on page 472
- clocking-mode on page 473
- community (Policy Options) on page 474
- compatibility-mode on page 477
- compression (PPP Properties) on page 478
- compression (Voice Services) on page 479
- compression-device on page 480
- connections on page 480
- connection-protection-tlv on page 481
- connectivity-fault-management on page 482
- container-devices on page 484
- container-list on page 485
- container-options on page 486
- container-type on page 487
- continuity-check on page 488
- control-channel on page 489
- control-polarity on page 490
- control-signal on page 491
- copy-tos-to-outer-ip-header on page 492
- core-dump on page 492
- crc-major-alarm-threshold on page 493
• crc-minor-alarm-threshold on page 494
• cts on page 495
• cts-polarity on page 496
• cycle-time on page 497
• damping (Interfaces) on page 498
• data-channel on page 500
• data-tlv-size on page 501
• dcd on page 502
• dcd-polarity on page 503
• dce on page 503
• deactivation-delay on page 504
• dce-options on page 505
• default-actions on page 506
• default-chap-secret on page 507
• default-pap-password on page 508
• delimiter on page 508
• demux-destination (Underlying Interface) on page 509
• demux-destination (Demux Interface) on page 510
• demux-options (Static Interface) on page 511
• demux-source (Demux Interface) on page 512
• demux-source (Underlying Interface) on page 513
• demux0 (Static Interface) on page 514
• demux0 (Dynamic Interface) on page 515
• description (Interfaces) on page 517
• destination (IPCP) on page 518
• destination (Routing Instance) on page 519
• destination (Tunnels) on page 520
• destination-class-usage on page 521
• destination-profile on page 522
• dial-options on page 523
• dial-string on page 524
• dialer on page 524
• dialer-options on page 525
• dialin on page 526
• direction on page 527
• disable (Interface) on page 528
• disable (Link Protection) on page 529
• disable-mlppp-inner-ppp-pfc on page 530
• dcli on page 531
• do-not-fragment on page 532
• domain-name on page 533
• dot1x on page 534
• down-count on page 535
• drop (PPPoE Service Name Tables) on page 536
• drop-timeout on page 537
• ds0-options on page 538
• dsl-options on page 539
• dsr on page 540
• dsr-polarity on page 541
• dte-options on page 542
• dtr on page 543
• dtr-circuit on page 544
• dtr-polarity on page 544
• dump-on-flow-control on page 545
• dynamic-call-admission-control on page 546
• dynamic-profile (PPP) on page 547
• dynamic-profile (PPPoE Service Name Tables) on page 548
• dynamic-profile (Stacked VLAN) on page 549
• dynamic-profile (VLAN) on page 550
• dynamic-profiles on page 551
• e1-options on page 562
• e3-options on page 563
• east-interface on page 564
• egress-policer-overhead on page 565
• encapsulation (Container Interface) on page 566
• encapsulation (Logical Interface) on page 567
• encapsulation on page 571
• encoding on page 579
• epd-threshold (Logical Interface) on page 580
• epd-threshold (Physical Interface) on page 581
• es-options on page 582
• ethernet (Protocols OAM) on page 583
• ethernet-policer-profile on page 589
• ethernet-ring on page 591
• ethernet-switch-profile on page 592
• eui-64 on page 594
• evcs on page 595
• event (LFM) on page 596
• event-thresholds on page 597
• fast-aps-switch on page 598
• f-max-period on page 599
• facility-override on page 599
• failover-delay on page 600
• family (Dynamic Standard Interface) on page 601
• family on page 603
• fastether-options on page 609
• fcs on page 610
• feac-loop-respond on page 611
• fec (gigether) on page 612
• filter on page 614
• filter (Applying to an Interface) on page 616
• flexible-vlan-tagging on page 617
• flow-control on page 618
• flow-control-options on page 619
• force on page 620
• forward-and-send-to-re on page 621
• forwarding-class (ATM2 IQ Scheduler Maps) on page 622
• forwarding-class (Gigabit Ethernet IQ Classifier) on page 623
• forward-only on page 624
• fragment-threshold on page 625
• frame-error on page 626
• frame-period on page 627
• frame-period-summary on page 628
• framing (E1, E3, and T1 Interfaces) on page 629
• framing (10-Gigabit Ethernet Interfaces) on page 630
• framing (SONET and SDH Interfaces) on page 631
• gigether-options on page 632
• gratuitous-arp-reply on page 634
• guard-interval on page 635
• hardware-assisted-timestamping on page 636
• high-plp-threshold on page 637
• hello-timer on page 638
• hierarchical-policer on page 639
• hierarchical-scheduler (Subscriber Interfaces on MX Series Routers) on page 640
• high-plp-max-threshold on page 641
• high-plp-threshold on page 642
• hold-interval (OAM) on page 643
• hold-interval (Protection Group) on page 644
• hold-time (APS) on page 645
• hold-time (Physical Interface) on page 646
• hold-time (SONET/SDH Defect Triggers) on page 648
• host (Interfaces) on page 649
• host-prefix-only on page 650
• iccp on page 651
• idle-cycle-flag on page 653
• idle-timeout on page 654
• ieee802.1p on page 655
• if-exceeding (Hierarchical Policer) on page 656
• if-exceeding-pps (Hierarchical Policer) on page 657
• igmp-snooping on page 658
• ignore on page 663
• ignore-all on page 663
• ignore-l3-incompletes on page 664
• ilmi on page 664
• ima-group-options on page 665
• ima-link-options on page 667
• inactivity-timeout on page 667
• incoming-map on page 668
• indication on page 669
• indication-polarity on page 670
• ingress-policer-overhead on page 671
• ingress-rate-limit on page 673
• init-command-string on page 674
• initial-route-check on page 675
• inner-tag-protocol-id on page 676
• inner-vlan-id on page 677
• inner-vlan-id-range on page 678
• input on page 679
- input-list on page 680
- input-policer on page 681
- input-priority-map on page 682
- input-three-color on page 683
- input-vlan-map (Aggregated Ethernet) on page 684
- input-vlan-map on page 685
- instance on page 686
- interface (Hierarchical CoS Schedulers) on page 686
- interface (IEEE 802.1x) on page 687
- interface (IEEE 802.1ag OAM Connectivity-Fault Management) on page 689
- interface (OAM Link-Fault Management) on page 690
- interface (Port Mirroring) on page 691
- interface-down on page 691
- interface-name on page 692
- interface-none on page 692
- interface-range on page 693
- interface-transmit-statistics on page 694
- interface-set (Ethernet Interfaces) on page 695
- interface-set (IP Demux Interfaces) on page 696
- interface-shared-with on page 697
- interface-status-tlv on page 698
- interface-switch on page 699
- interface-type (Interfaces) on page 700
- interfaces on page 702
- interfaces (Static and Dynamic Subscribers) on page 703
- interleave-fragments on page 709
- interval on page 710
- inverse-arp on page 711
- invert-data on page 712
- ipsec-sa on page 713
- isdn-options on page 714
- iteration-count on page 715
- iteration-period on page 716
- keep-address-and-control on page 717
- keepalives on page 718
- key on page 719
- l2tp-interface-id on page 720
• lACP (Protocols) on page 721
• lACP (802.3ad) on page 722
• lACP (Aggregated Ethernet) on page 723
• Layer2-policer on page 726
• lcp-max-conf-req on page 727
• lcp-restart-timer on page 728
• Level on page 729
• line-encoding on page 730
• line-protocol on page 731
• line-rate on page 732
• linear-red-profile on page 733
• linear-red-profiles on page 734
• link-adjacency-loss on page 735
• link-discovery on page 735
• link-down on page 736
• link-event-rate on page 736
• link-fault-management on page 737
• link-layer-overhead on page 738
• link-mode on page 739
• link-protection on page 741
• link-speed (Aggregated Ethernet) on page 742
• link-speed (Aggregated SONET/SDH) on page 744
• linktrace on page 745
• Lmi (Frame Relay) on page 746
• Lmi (Ethernet OAM) on page 748
• Lmi-type on page 749
• load-interval on page 750
• load-threshold on page 751
• local-name on page 752
• local-password on page 753
• lockout on page 753
• log-prefix (Interfaces) on page 754
• logical-interface-fpc-redundancy (Aggregated Ethernet Subscriber Interfaces) on page 754
• logical-interface-policer on page 755
• logical-systems on page 757
• long-buildout on page 758
• loop-timing on page 759
• loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3) on page 760
• loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet) on page 762
• loopback (Serial) on page 763
• loopback-clear-timer on page 764
• loss-priority on page 765
• loss-threshold on page 766
• low-plp-max-threshold on page 767
• low-plp-threshold on page 768
• lowest-priority-defect on page 769
• lsq-failure-options on page 770
• mac on page 771
• mac-address (Accept Source Mac) on page 772
• mac-address (VLAN and Stacked VLAN Interfaces) on page 773
• mac-learn-enable on page 774
• mac-validate on page 775
• maintenance-association on page 776
• maintenance-domain on page 777
• master-only on page 778
• maximum-contexts on page 779
• maximum-requests on page 780
• maximum-vcs on page 781
• mc-ae on page 782
• member-interface-speed on page 785
• member-interface-type on page 786
• mep on page 787
• minimum-links on page 788
• mip-half-function on page 789
• mlfr-uni-nni-bundle-options on page 790
• mode (Dynamic Profiles) on page 791
• mode (Interfaces) on page 792
• modem-options on page 793
• monitor-session on page 794
• mpls (Interfaces) on page 795
• mrru on page 796
• mtu on page 797
• multi-chassis-protection on page 801
• multicast-dci on page 802
• multicast-only on page 803
• multicast-statistics on page 804
• multicast-vci on page 805
• multilink-max-classes on page 806
• multipoint on page 806
• multipoint-destination on page 807
• multiservice-options on page 808
• n391 on page 809
• n392 on page 810
• n393 on page 811
• name-format on page 812
• native-vlan-id on page 813
• ncp-max-conf-req on page 815
• ncp-restart-timer on page 816
• nd6-stale-time on page 817
• negotiate-address on page 818
• negotiation-options on page 819
• neighbor (Automatic Protection Switching for SONET/SDH) on page 820
• no-allow-link-events on page 820
• no-aggregate-delegate-processing on page 821
• asynchronous-notification on page 822
• no-auto-mdix on page 823
• auto-negotiation on page 824
• cbit-parity on page 826
• core-dump on page 827
• feac-loop-respond on page 828
• flow-control on page 829
• gratuitous-arp-reply on page 830
• no-gratuitous-arp-request on page 831
• no-keepalives on page 832
• long-buildout on page 833
• loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet) on page 834
• mac-learn-enable on page 835
• no-partition on page 836
• payload-scrambler on page 838
• no-pre-classifier on page 839
• no-redirects on page 840
• source-filtering on page 841
• syslog (Monitoring) on page 842
• no-termination-request on page 843
• translate-discard-eligible on page 844
• translate-fecn-and-becn on page 844
• unframed on page 845
• z0-increment on page 845
• node-id on page 846
• non-revertive (Interfaces) on page 846
• oam on page 847
• oam-liveness on page 850
• oam-period on page 851
• oc-slice on page 852
• open-timeout on page 853
• operating-mode on page 854
• optics-options on page 855
• option-82 on page 856
• otn-options on page 857
• output on page 859
• output-list on page 860
• output-policer on page 861
• output-priority-map on page 862
• output-three-color on page 863
• output-vlan-map (Aggregated Ethernet) on page 864
• output-vlan-map on page 865
• overflow (Receive Bucket) on page 866
• overflow (Transmit Bucket) on page 866
• override on page 867
• pado-advertise on page 868
• paired-group on page 869
• pap on page 870
• partition on page 871
• passive (CHAP) on page 872
• passive (PAP) on page 873
• passive-monitor-mode on page 874
• password (Interfaces) on page 875
• path-database-size on page 875
• path-trace on page 876
• payload-scrambler on page 877
• payload-size on page 878
• pdu-interval on page 879
• pdu-threshold on page 880
• peer on page 881
• peer-unit on page 882
• per-unit-scheduler on page 883
• performance-monitoring on page 885
• periodic on page 886
• pfc on page 887
• pic-type on page 887
• plp-to-clp on page 888
• plp1 on page 889
• point-to-point on page 890
• policer (CFM Firewall) on page 891
• policer (CFM Global) on page 892
• policer (CFM Session) on page 893
• policer (CoS) on page 894
• policer (Interface) on page 895
• policer (MAC) on page 896
• policy-statement on page 897
• pool on page 901
• pop on page 902
• pop-all-labels on page 903
• pop-pop on page 904
• pop-swap on page 905
• port on page 906
• port-priority on page 907
• port-status-tlv on page 908
• post-service-filter on page 909
• ppp-options on page 910
• pppoe-options on page 912
• pppoe-underlying-options (Static and Dynamic Subscribers) on page 913
• preferred on page 914
• preferred-source-address on page 915
- preferred-source-address on page 916
- premium (Hierarchical Policer) on page 918
- premium (Output Priority Map) on page 919
- premium (Policer) on page 920
- preserve-interface on page 921
- primary (Address on Interface) on page 922
- primary (Interface for Router) on page 923
- primary (AS PIC or Multiservices PIC Interfaces) on page 924
- priority (OAM Connectivity-Fault Management) on page 925
- priority (Schedulers) on page 926
- promiscuous-mode on page 927
- protect-circuit on page 928
- protection-group on page 929
- protocol-down on page 931
- protocols on page 932
- proxy on page 933
- proxy-arp on page 934
- push on page 935
- push-push on page 936
- queue-depth on page 937
- queue-length on page 938
- queues on page 939
- quiet-period on page 940
- radius-realm on page 941
- ranges (Dynamic Stacked VLAN) on page 942
- ranges (Dynamic VLAN) on page 943
- rate on page 944
- rate on page 945
- rdi on page 945
- reassemble-packets on page 946
- reauthentication on page 947
- receive-bucket on page 948
- receive-options-packets on page 949
- receive-ttl-exceeded on page 949
- red-differential-delay on page 950
- redial-delay on page 951
- redundancy-options on page 952
• remote on page 953
• remote-loopback on page 954
• remote-loopback-respond on page 955
• remote-mep on page 956
• remove-when-no-subscribers on page 957
• request on page 957
• required-depth on page 958
• restore-interval on page 959
• retries on page 960
• revert-time (Interfaces) on page 961
• revertive on page 962
• rfc-2615 on page 963
• ring-protection-link-end on page 963
• ring-protection-link-owner on page 964
• routing-instance on page 965
• routing-instance (PPPoE Service Name Tables) on page 966
• rpf-check (Dynamic Profiles) on page 967
• rpf-check on page 968
• rpf-loose-mode-discard on page 969
• rtp on page 970
• rts on page 971
• rts-polarity on page 972
• rtvbr on page 973
• sa-multicast (100-Gigabit Ethernet) on page 975
• sampling (Interfaces) on page 976
• satop-options on page 977
• shared-interface on page 978
• scheduler-maps (For ATM2 IQ Interfaces) on page 979
• schedulers on page 980
• secondary on page 980
• send-critical-event on page 981
• serial-options on page 982
• server on page 983
• server-timeout on page 984
• service (Logical Interfaces) on page 985
• service (PPPoE) on page 986
• service-domain on page 987
• switching-mode on page 1031
• symbol-period on page 1032
• syslog (Interfaces) on page 1033
• syslog (Monitoring) on page 1034
• syslog (OAM Action) on page 1035
• system-priority on page 1036
• t1-options on page 1037
• t310 on page 1038
• t391 on page 1039
• t392 on page 1040
• t3-options on page 1041
• tag-protocol-id (TPIDs Expected to Be Sent or Received) on page 1042
• tag-protocol-id (TPID to Rewrite) on page 1043
• targeted-broadcast on page 1044
• targeted-distribution (Static Interfaces over Aggregated Ethernet) on page 1045
• tei-option on page 1046
• terminate (PPPoE Service Name Tables) on page 1047
• then on page 1048
• threshold on page 1049
• timeslots on page 1050
• tm on page 1051
• tm-polarity on page 1052
• traceoptions (Individual Interfaces) on page 1053
• traceoptions (Individual Interfaces) on page 1060
• traceoptions (LACP) on page 1067
• traceoptions (PPP Process) on page 1069
• traceoptions (PPPoE) on page 1072
• translate-discard-eligible on page 1074
• translate-fecn-and-becn on page 1075
• translate-plp-control-word-de on page 1075
• transmit-bucket on page 1076
• transmit-clock on page 1077
• transmit-period on page 1078
• transmit-weight (ATM2 IQ CoS Forwarding Class) on page 1079
• transmit-weight (ATM2 IQ Virtual Circuit) on page 1080
• traps on page 1081
• trigger on page 1082
- vlan-vci-tagging on page 1137
- vpi (ATM CCC Cell-Relay Promiscuous Mode) on page 1137
- vpi (Define Virtual Path) on page 1138
- vpi (Logical Interface and Interworking) on page 1139
- vtmapping on page 1140
- warning on page 1141
- watch-list on page 1142
- wavelength on page 1143
- west-interface on page 1147
- working-circuit on page 1148
- yellow-differential-delay on page 1149
- z0-increment on page 1150
802.3ad

Syntax

```plaintext
802.3ad {
    primary | backup;
    ae interface-number ;
    lacp {
        port-priority priority-number;
    }
    link-index index-number
    distribution-list distribution-list-number
}
```

Hierarchy Level

```plaintext
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]
```

Release Information

Statement introduced before Junos OS Release 7.4. 
**primary** and **backup** options added in Junos OS Release 8.3.

Description

Specify aggregated Ethernet logical interface number.

Options

- **bundle**—Join an aggregated Ethernet interface.
  ```plaintext
  ae interface-number — Aggregated Ethernet logical interface number. For MX Series routers running Junos release 14.2R3 and later you can configure a maximum of 1000 aggregated interfaces. On MX2010 and MX2020 routers you can configure a maximum of 800 aggregated interfaces.
  
  primary | backup — For link protection configurations, specify the link as primary link or backup link for egress traffic.
  
  lacp — Configure Link Aggregation Control Protocol. Specify the port priority in the range 0 through 65535. Default port-priority is 127.
  ```

- **link-index**—Specify the desired child link index within the aggregated Ethernet Interface. Index number of the logical interface reflects its initialization sequence.

- **distribution-list**—For targeted distribution, specify the distribution list to which the interface belongs.

Required Privilege Level

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

Related Documentation

- Configuring an Aggregated Ethernet Interface
- Configuring Aggregated Ethernet Link Protection
Syntax  accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);

Hierarchy Level  [edit interfaces interface-name auto-configure stacked-vlan-ranges dynamic-profile profile-name],
[edit interfaces interface-name auto-configure vlan-ranges dynamic-profile profile-name]

Release Information  Statement introduced in Junos OS Release 9.5.
dhcp-v4 option added in Junos OS Release 10.0.
dhcp-v6, inet6 and pppoe options added in Junos OS Release 10.2.
any option added in Junos OS Release 10.4.

Description  Specify the type of VLAN Ethernet packet accepted by an interface that is associated with a VLAN dynamic profile or stacked VLAN dynamic profile.

Options

any—Any packet type. Specifies that any incoming packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes. This option is used when configuring wholesaling in a Layer 2 network.

dhcp-v4—IPv4 DHCP packet type. Specifies that incoming IPv4 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes.

NOTE: The DHCP-specific mac-address and option-82 options are rejected if the accept statement is not set to dhcp-v4.

dhcp-v6—IPv6 DHCP packet type. Specifies that incoming IPv6 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes.

inet—IPv4 Ethernet and ARP packet type.

inet6—IPv6 Ethernet packet type.

pppoe—Point-to-Point Protocol over Ethernet packet type.

NOTE: The pppoe VLAN Ethernet packet type option is supported only for MPC/MIC interfaces.
### Required Privilege Level
- *interface*—To view this statement in the configuration.
- *interface-control*—To add this statement to the configuration.

### Related Documentation
- Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs
- Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution
- Configuring Subscriber Packet Types to Trigger VLAN Authentication
accept-source-mac

Syntax

```
accept-source-mac {
  mac-address mac-address {
    policer {
      input cos-policer-name;
      output cos-policer-name;
    }
  }
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

For Gigabit Ethernet intelligent queuing (IQ) interfaces only, accept traffic from and to the specified remote media access control (MAC) address.

The `accept-source-mac` statement is equivalent to the `source-address-filter` statement, which is valid for aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only. To allow the interface to receive packets from specific MAC addresses, include the `accept-source-mac` statement.

On untagged Gigabit Ethernet interfaces, you should not configure the `source-address-filter` statement and the `accept-source-mac` statement simultaneously. On tagged Gigabit Ethernet interfaces, you should not configure the `source-address-filter` statement and the `accept-source-mac` statement with an identical MAC address specified in both filters.

The remaining statements are explained separately. See CLI Explorer.

**NOTE:** The policer statement is not supported on PTX Series Packet Transport Routers.

**NOTE:** On QFX platforms, if you configure source MAC addresses for an interface using the `static-mac` or `persistent-learning` statements and later configure a different MAC address for the same interface using the `accept-source-mac` statement, the MAC addresses that you previously configured for the interface remain in the ethernet-switching table and can still be used to send packets to the interface.
<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interface—To view this statement in the configuration.</td>
<td></td>
</tr>
<tr>
<td>interface-control—To add this statement to the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Documentation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring MAC Address Filtering</td>
<td></td>
</tr>
<tr>
<td>Configuring MAC Address Filtering on PTX Series Packet Transport Routers</td>
<td></td>
</tr>
<tr>
<td>source-filtering on page 841</td>
<td></td>
</tr>
</tbody>
</table>
access-concentrator

Syntax

access-concentrator name;

Hierarchy Level

/edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family pppoe],
/edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family pppoe],
/edit interfaces interface-name unit logical-unit-number family pppoe],
/edit interfaces interface-name unit logical-unit-number pppoe-options],
/edit interfaces interface-name unit logical-unit-number pppoe-underlying-options],
/edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family pppoe],
/edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number pppoe-options],
/edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number pppoe-underlying-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Support at the [edit interfaces interface-name unit logical-unit-number pppoe-underlying-options] and [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number pppoe-underlying-options] hierarchy levels introduced in Junos OS Release 10.1.
Support at the [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.

Description

Configure an alternative access concentrator name in the AC-NAME tag in a PPPoE control packet for use with a dynamic PPPoE subscriber interface. If you do not configure the access concentrator name, the AC-NAME tag contains the system name.

NOTE: The [edit ... family pppoe] hierarchies are supported only on MX Series routers with MPCs.

Options

name—Name of the access concentrator.

Required Privilege Level

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

Related Documentation

- Identifying the Access Concentrator
- Configuring the PPPoE Family for an Underlying Interface
- Configuring Dynamic PPPoE Subscriber Interfaces
- PPPoE Overview
**access-profile**

**Syntax**

```
access-profile name;
```

**Hierarchy Level**

```
[edit interfaces interface-name ppp-options chap],
[edit interfaces interface-name ppp-options pap],
[edit interfaces interface-name unit logical-unit-number ppp-options chap],
[edit interfaces interface-name unit logical-unit-number ppp-options pap],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options chap],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options pap]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Support for PAP added in Junos OS Release 8.3.
Support for VLAN and stacked VLAN ranges added in Junos OS Release 10.0.

**Description**

For CHAP authentication, the mapping between peer names (or “clients”) and the secrets associated with their respective links. For PAP authentication, the peer’s username and password.

For Asynchronous Transfer Mode 2 (ATM2) IQ interfaces only, you can configure a Challenge Handshake Authentication Protocol (CHAP) access profile on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- **atm-ppp-llc**—PPP over AAL5 logical link control (LLC) encapsulation.
- **atm-ppp-vc-mux**—PPP over AAL5 multiplex encapsulation.

**Options**

- `name`—Name of the access profile.

**Required Privilege Level**

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

**Related Documentation**

- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
- Configuring the PPP Password Authentication Protocol On a Physical Interface on page 124
accounting

Syntax
accounting {
   destination-class-usage;
   source-class-usage {
      direction;
   }
}

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Enable IP packet counters on an interface.
The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- Enabling Source Class and Destination Class Usage on page 241
accounting-profile

**Syntax**

```
accounting-profile name;
```

**Hierarchy Level**

```
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-range 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**

Enable collection of accounting data for the specified physical or logical interface or interface range.

**Options**

* name—Name of the accounting profile.

**Required Privilege**

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

**Related Documentation**

* Applying an Accounting Profile to the Physical Interface
* Applying an Accounting Profile to the Logical Interface
acfc

Syntax acfc;

Hierarchy Level [edit interfaces interface-name ppp-options compression],
[edit interfaces interface-name unit logical-unit-number ppp-options compression],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options compression]

Release Information Statement introduced before Junos OS Release 7.4.

Description For interfaces with PPP encapsulation, configure compression of the Data Link Layer address and control fields. The acfc option is not supported with frame-relay-ppp encapsulation.

On M320, M120, and T Series routers, address and control field compression (ACFC) is not supported for any ISO family protocols. Do not include the acfc statement at the [edit interfaces interface-name ppp-options compression] hierarchy level when you include the family iso statement at the [edit interfaces interface-name unit logical-unit-number] 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 PPP Address and Control Field Compression on page 133
**Syntax**

acknowledge-retries number;

**Hierarchy Level**

[edit interfaces interface-name mfr-uni-nni-bundle-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For link services and voice services interfaces only, configure the number of retransmission attempts to be made for consecutive hello or remove link messages following the expiration of the acknowledgment timer.

**Options**

- **number**—Number of retransmission attempts to be made following the expiration of the acknowledgment timer.
  - **Range:** 1 through 5
  - **Default:** 2

**Required Privilege**

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

**Related Documentation**

- Junos OS Services Interfaces Library for Routing Devices
- action-red-differential-delay on page 404
- hello-timer on page 638
acknowledge-timer

Syntax

acknowledge-timer milliseconds;

Hierarchy Level [edit interfaces interface-name mllfr-uni-nni-bundle-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For link services and voice services interfaces only, configure the maximum time, in milliseconds, to wait for an add link acknowledgment, hello acknowledgment, or remove link acknowledgment message.

Options milliseconds—Time, in milliseconds, to wait for an add link acknowledgment, hello acknowledgment, or remove link acknowledgment message.

Range: 1 through 10 milliseconds
Default: 4 milliseconds

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

Related Documentation • Junos OS Services Interfaces Library for Routing Devices
• address on page 407, hello-timer on page 638
• hello-timer on page 638
**action (OAM)**

**Syntax**
```
action {
  link-down;
  send-critical-event;
  syslog;
}
```

**Hierarchy Level**
```
[edit protocols oam ethernet link-fault-management action-profile]
```

**Release Information**
Statement introduced in Junos OS Release 8.5.

**Description**
Define the action or actions to be taken when the OAM fault event occurs.

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

**Related Documentation**
- *Specifying the Actions to Be Taken for Link-Fault Management Events*

---

**action (Policer)**

**Syntax**
```
action {
  loss-priority high then discard;
}
```

**Hierarchy Level**
```
[edit firewall three-color-policer policer-name]
```

**Release Information**
Statement introduced in Junos OS Release 8.2.

**Description**
This statement discards high loss priority traffic as part of a configuration using tricolor marking on a logical interface.

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

**Related Documentation**
- *Class of Service Feature Guide (Routers and EX9200 Switches)*
- *logical-interface-policer on page 755*
**action-profile (Applying to CFM)**

Syntax

```
action-profile profile-name;
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name mep mep-id remote-mep mep-id]
```

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Identify the action profile to use.

Options

```
profile-name—Name of the action profile to use.
```

Required Privilege

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

Related Documentation

- Configuring a MEP to Generate and Respond to CFM Protocol Messages
action-profile (Defining for CFM)

Syntax  
```
action-profile profile-name {
  event {
    ais-trigger-condition {
      adjacency-loss;
      all-defects;
      cross-connect-ccm;
      erroneous-ccm;
      receive-ais;
    }
    interface-status-tlv (down | lower-layer-down);
    port-status-tlv blocked;
    rdi;
  }
  action {
    interface-down;
    log-and-generate-ais {
      interval(1m | 1s);
      level value;
      priority value;
    }
  }
  default-actions {
    interface-down;
  }
}
```

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management]

Release Information  
Statement introduced in Junos OS Release 8.4.

Description  
Configure a name and default action for an action profile.

Options  
`profile-name`—Name of the action 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 a CFM Action Profile to Specify CFM Actions for CFM Events
- default-actions on page 506
- event (CFM)
- interface-down on page 691
action-profile

List of Syntax  Syntax: T, M, MX and ACX Series Routers, SRX Series Firewalls and EX Series Switches on page 403
Syntax: EX Series Switches and NFX Series Devices on page 403

Syntax: T, M, MX and ACX Series Routers, SRX Series Firewalls and EX Series Switches  action-profile profile-name {  action {    link-down;    send-critical-event;    syslog;  }  event {    link-adjacency-loss;    link-event-rate {      frame-error count;      frame-period count;      frame-period-summary count;      symbol-period count;    }    protocol-down;  } }

Syntax: EX Series Switches and NFX Series Devices  action-profile profile-name;  action {    syslog;    link-down;  }  event {    link-adjacency-loss;    link-event-rate {      frame-error count;      frame-period count;      frame-period-summary count;      symbol-period count;    }  }

Hierarchy Level  [edit protocols oam ethernet link-fault-management]

Release Information  Statement introduced in Junos OS Release 8.5 for T, M, MX and ACX Series Routers, SRX Series Firewalls, and EX Series Switches.
Statement introduced in Junos OS Release 9.4 for EX Series switches and NFX Series devices.

Description  Configure an Ethernet OAM link fault management (LFM) action profile by specifying a profile name.
The remaining statements are explained separately. See CLI Explorer.

Options  
- **profile-name**—Name of the action profile.

The remaining statements are explained separately. See CLI Explorer.

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

**Related Documentation**  
- Configuring an OAM Action Profile  
- Configuring Ethernet OAM Link Fault Management

---

**action-red-differential-delay**

**Syntax**  
`action-red-differential-delay (disable-tx | remove-link);`

**Hierarchy Level**  
[edit interfaces interface-name mfr-uni-nni-bundle-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For link services and voice services interfaces only, configure the action to be taken when the differential delay exceeds the red limit.

**Options**  
- **disable-tx**—Disable transmission on the bundle link.
- **remove-link**—Remove bundle link from service.
  
  Default: disable-tx

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

**Related Documentation**  
- Junos OS Services Interfaces Library for Routing Devices  
- remote on page 953  
- yellow-differential-delay on page 1149
**activation-delay**

**Syntax**

activation-delay seconds;

**Hierarchy Level**

[edit interfaces dln unit logical-unit-number dialer-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

(J Series Services Routers) For ISDN interfaces, configure the ISDN dialer activation delay. Used only for dialer backup and dialer watch cases.

**Options**

seconds—Interval before the backup interface is activated after the primary interface has gone down.

**Range:** 1 through 4,294,967,295 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 Interfaces and Routing Configuration Guide
activation-priority

Syntax  
activation-priority priority;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number dynamic-call-admission-control],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number  
dynamic-call-admission-control]

Release Information  
Statement introduced in Junos OS Release 8.2.

Description  
(J4350 and J6350 Services Routers supporting voice over IP with the TGM550 media  
gateway module) For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces,  
and serial interfaces with PPP or Frame Relay encapsulation, configure the dynamic call  
admission control (dynamic CAC) activation priority value.

Options  
priority—The activation priority in which the interface is used for providing call bandwidth.  
The interface with the highest activation priority value is used as the primary link for  
providing call bandwidth. If the primary link becomes unavailable, the TGM550  
switches over to the next active interface with the highest activation priority value,  
and so on.  
Range: 0 through 255  
Default: 50

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

Related Documentation  
• Junos OS Services Interfaces Library for Routing Devices  
• Junos OS Interfaces and Routing Configuration Guide
address

Syntax

```
adddess address [  
  arp ip-address (mac | multicast-mac) mac-address <publish>;  
  broadcast address;  
  destination address;  
  destination-profile name;  
  eui-64;  
  master-only;  
  multipoint-destination address dlci dlci-identifier;  
  multipoint-destination address {  
    epd-threshold cells;  
    inverse-arp;  
    oam-liveness {  
      up-count cells;  
      down-count cells;  
    }  
    oam-period (disable | seconds);  
    shaping {  
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);  
      queue-length number;  
    }  
  vci vpi-identifier.vci-identifier;  
  }  
  primary;  
  preferred;  
  virtual-gateway-address  
  (vrrp-group | vrrp-inet6-group) group-number [  
    (accept-data | no-accept-data);  
    advertise-interval seconds;  
    authentication-type authentication;  
    authentication-key key;  
    fast-interval milliseconds;  
    (preempt | no-preempt) {  
      hold-time seconds;  
    }  
    priority-number number;  
    track {  
      priority-cost seconds;  
      priority-hold-time interface-name [  
        interface priority;  
        bandwidth-threshold bits-per-second {  
          priority;  
        }  
      }  
    route ip-address/mask routing-instance instance-name priority-cost cost;  
  }  
  virtual-address [ addresses ];  
}  
```
**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number family family],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Configure the interface address.

---

**NOTE:** If you configure the same address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration, and the remaining address configurations are ignored and can leave interfaces without an address. Interfaces that do not have an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

For example, in the following configuration the address configuration of interface xe-0/0/1.0 is ignored:

```
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/8;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
      family inet {
        address 192.168.1.1/8;
      }
    }
  }
}
```

For more information on configuring the same address on multiple interfaces, see "Configuring the Interface Address" on page 191.

- In Junos OS Release 13.3 and later, when you configure an IPv6 host address and an IPv6 subnet address on an interface, the commit operation fails.
- In releases earlier than Junos OS Release 13.3, when you use the same configuration on an interface, the commit operation succeeds, but only one of the IPv6 addresses that was entered is assigned to the interface. The other address is not applied.
Options  
- **address**—Address of the interface.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

---

**NOTE:** The edit logical-systems hierarchy is not available on QFabric systems.

---

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

**Related Documentation**
- Configuring the Protocol Family on page 190
- `family`
- `negotiate-address on page 818`
- `unnumbered-address (Ethernet) on page 1107`

---

**advertise-interval**

**Syntax**
```adventer-interval milliseconds;```

**Hierarchy Level**
```
[edit interfaces interface-name sonet-options aps]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Modify the Automatic Protection Switching (APS) interval at which the protect and working routers send packets to their neighbors to advertise that they are operational. A router considers its neighbor to be operational for a period, called the hold time, that is, by default, three times the advertisement interval.

**Options**
- **milliseconds**—Interval between advertisement packets.
  - **Range:** 1 through 65,534 milliseconds
  - **Default:** 1000 milliseconds

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

**Related Documentation**
- Configuring APS Timers
**age**

**Syntax**

```
age (30m | 10m | 1m | 30s | 10s);
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management linktrace]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.

**Description**

Time to wait (in minutes or seconds) for a response. If no response is received, the request and response entry is deleted from the linktrace database.

**Default**

10 minutes

**Required Privilege**

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

**Related Documentation**

- Configuring Linktrace Protocol in CFM
agent-specifier

Syntax

agent-specifier {  
  aci circuit-id-string ari remote-id-string {  
    drop;  
    delay seconds;  
    terminate;  
    dynamic-profile profile-name;  
    routing-instance routing-instance-name;  
    static-interface interface-name;  
  }  
}

Hierarchy Level
[edit protocols pppoe service-name-tables table-name service service-name]

Release Information
Statement introduced in Junos OS Release 10.0. drop, delay, terminate, dynamic-profile, routing-instance, and static-interface options introduced in Junos OS Release 10.2.

Description
Specify the action taken by the interface for the specified agent circuit identifier/agent remote identifier (ACI/ARI) pair when the interface receives a PPPoE Active Discovery Initiation (PADI) control packet that includes the vendor-specific tag with ACI/ARI pair information. You can configure an ACI/ARI pair for a named service, empty service, or any service in a PPPoE service name table. A maximum of 8000 ACI/ARI pairs are supported per PPPoE service name table. You can distribute the ACI/ARI pairs in any combination among the named, empty, and any service entries in the service name table.

You can use an asterisk (*) as a wildcard character to match ACI/ARI pairs, the ACI alone, or the ARI alone. The asterisk can be placed only at the beginning, the end, or both the beginning and end of the identifier string. You can also specify an asterisk alone for either the ACI or the ARI. You cannot specify only an asterisk for both the ACI and the ARI. When you specify a single asterisk as the identifier, that identifier is ignored in the PADI packet.

For example, suppose you care about matching only the ACI and do not care what value the ARI has in the PADI packet, or even whether the packet contains an ARI value. In this case you can set the remote-id-string to a single asterisk. Then the interface ignores the ARI received in the packet and the interface takes action based only on matching the specified ACI.

Default
The default action is terminate.

Options
aci circuit-id-string—Identifier for the agent circuit ID that corresponds to the DSLAM interface that initiated the service request. This is a string of up to 63 characters.

ari remote-id-string—Identifier for the subscriber associated with the DSLAM interface that initiated the service request. This is a string of up to 63 characters.
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**
- Interface—To view this statement in the configuration.
- Interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring PPPoE Service Name Tables
- Assigning an ACI/ARI Pair to a Service Name and Configuring the Action Taken When the Client Request Includes ACI/ARI Information

### aggregate (Gigabit Ethernet CoS Policier)

**Syntax**
```plaintext
aggregate {
  bandwidth-limit bps;
  burst-size-limit bytes;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Define a policer to apply to nonpremium traffic.

The remaining statements are explained separately. See CLI Explorer.

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

**Related Documentation**
- Configuring Gigabit Ethernet Policers
- premium (Hierarchical Policier) on page 918
- ieee802.1p on page 655
aggregate (Hierarchical Policer)

Syntax

```
aggregate {
  if-exceeding {
    bandwidth-limit bandwidth;
    burst-size-limit burst;
  }
  then {
    discard;
  }
}
```

Hierarchy Level  [edit firewall hierarchical-policer]

Release Information  Statement introduced in Junos OS Release 9.5.

Description  On M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, T4000 routers with Type 5 FPC and Enhanced Scaling Type 4 FPC, configure an aggregate hierarchical policer.

Options  Options are described separately.

Required Privilege Level  firewall—To view this statement in the configuration.

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

Related Documentation  • Applying Policers on page 210

• Class of Service Feature Guide (Routers and EX9200 Switches)
aggregate (SONET/SDH)

Syntax  
aggregate asx;

Hierarchy Level  
[edit interfaces interface-name sonet-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Specify aggregated SONET/SDH logical interface number.

Options  
asx—Aggregated SONET/SDH logical interface number.
Range: 0 through 15

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

Related Documentation  
• Configuring Aggregated SONET/SDH Interfaces

aggregate-ports

Syntax  
aggregate-ports;

Hierarchy Level  
[edit chassis fpc slot-number pic pic-number]

Release Information  
Statement introduced in Junos OS Release 8.1.

Description  
For T Series routers only, specify OC768-over-OC192 mode on the 4-port OC192C PIC. Four OC192 links are aggregated into one OC768 link with one logical interface.

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

Related Documentation  
• Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode
aggregated-ether-options

Syntax
aggregated-ether-options {
    ethernet-switch-profile {
        ethernet-policer-profile {
            input-priority-map {
                ieee802.1p premium [ values ];
            }
            output-priority-map {
                classifier {
                    premium {
                        forwarding-class class-name {
                            loss-priority (high | low);
                        }
                    }
                }
            }
        }
    }
    policer cos-policer-name {
        aggregate {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        premium {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
    }
    (mac-learn-enable | no-mac-learn-enable);
} (flow-control | no-flow-control);
lacp {
    (active | passive);
    link-protection {
        disable;
        (revertive | non-revertive);
        periodic interval;
        system-priority priority;
        system-id system-id;
    }
} load-balance {
    local-bias;
    no-adaptive;
    per-packet;
}
local-bias;
link-speed speed;
logical-interface-chassis-redundancy;
logical-interface-fpc-redundancy;
(loopback | no-loopback);
minimum-links number;
rebalance-periodic time hour:minute <interval hours>;
source-address-filter {
mac-address;
(source-filtering | no-source-filtering);
}
}

Hierarchy Level  [edit interfaces aex]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure aggregated Ethernet-specific interface properties.

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  •  Ethernet Interfaces Overview

aggregated-sonet-options

generated-sonet-options {
  link-speed speed;
  minimum-links number;
}

Hierarchy Level  [edit interfaces asx]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure aggregated SONET/SDH-specific interface properties.

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 Aggregated SONET/SDH Interfaces
alarm (optics-options)

Syntax    alarm low-light–alarm {
            (link-down | syslog);
        }

Hierarchy Level    [edit interfaces interface-name optics-options]

Release Information    Statement introduced in Junos OS Release 10.0.
                        Statement introduced in Junos OS Release 12.1 for EX Series switches.
                        Statement introduced in Junos OS Release 18.3R1 for PTX10K-LC1104 on the PTX10008
                        and PTX10016 routers.

Description    Specify the action to take if the receiving optics signal is below the optics low-light alarm
                threshold.

Options    link-down—Drop the 10-Gigabit Ethernet link and marks link as down.
            syslog—Write the optics information to the system log.

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

Related Documentation    • Configuring Link Down Notification for Optics Options Alarm or Warning
                          • 100-Gigabit Ethernet OTN Options Configuration Overview
### alias (Interfaces)

**Syntax**

```
alias alias-name;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**

Statement introduced in Junos OS Release 13.3.

**Description**

Configure a textual description of a physical interface or the logical unit of an interface to be the alias of an interface name. The alias name can be a single line of text. If the text contains spaces, enclose it in quotation marks. If you configure an alias name, the alias name is displayed instead of the interface name in the output of all `show`, `show interfaces`, and other operational mode commands. In Junos OS Release 12.3R8 and later, display of the alias can be suppressed in favor of the actual interface name by using the `display no-interface-alias` parameter along with the show command.

**Options**

`alias-name`—Text to denote an easily identifiable, meaningful alias name for the interface. If the text includes spaces, enclose the entire text in quotation marks.

**Required Privilege Level**

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

**Related Documentation**

- Example: Adding an Interface Alias Name on page 108
- Junos OS Network Interfaces Library for Routing Devices
**allow-any-vci**

**Syntax**
`allow-any-vci;`

**Hierarchy Level**
- `[edit interfaces interface-name unit 0]`
- `[edit logical-systems logical-system-name interfaces interface-name unit 0]`

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro routers.

**Description**
Dedicate entire ATM device to ATM cell relay circuit.

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

**Related Documentation**
- *Configuring an ATM Cell-Relay Circuit Overview*
allow-fragmentation

Syntax

allow-fragmentation;

Hierarchy Level

edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel],
[edit logical-systems logical-system-name interfaces gr-fpc/pic/port unit logical-unit-number tunnel]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches.
Statement introduced in Junos OS Release 19.3 for MPC10E line card.

Description

For a generic routing encapsulation (GRE) tunnel, enable fragmentation of GRE-encapsulated packets whose size exceeds the maximum transmission unit (MTU) value of a link that the packet passes through. The don’t-fragment (DF) bit is not set in the outer IP header of GRE-encapsulated packets.

To enable the reassembly of fragmented GRE-encapsulated packets on GRE tunnel interfaces at the endpoint of the GRE tunnel, include the reassemble-packets statement for the interface.

NOTE: The reassemble-packets statement is not supported on MPC10E line card in Junos OS Release 19.3.

Default

If you do not include the allow-fragmentation statement, fragmentation of GRE-encapsulated packets is disabled.

Required Privilege Level

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

Related Documentation

- reassemble-packets
- Enabling Fragmentation and Reassembly on Packets After GRE-Encapsulation
- Junos OS Services Interfaces Library for Routing Devices
allow-remote-loopback

Syntax
allow-remote-loopback;

Hierarchy Level  [edit protocols oam link-fault-management interface interface-name negotiation-options]

Release Information  Statement introduced in Junos OS Release 8.4.

Description  Enable the remote loopback on IQ2 and IQ2-E Gigabit Ethernet interfaces, and Ethernet interfaces on the MX Series routers and EX Series switches.

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

Related Documentation  •  Enabling Remote Loopback Support on the Local Interface

annex

Syntax  annex (annex-a | annex-b);

Hierarchy Level  [edit interfaces interface-name shdsl-options],
[edit interfaces interface-name sonet-options aps],
[edit logical-systems logical-system-name interfaces interface-name shdsl-options]

Release Information  Statement introduced in Junos OS Release 7.4.

Description  For M320 and M120 routers only, for Multiplex Section Protection (MSP) switching on SDH interfaces, set annex-b. You must also configure the working protection circuit under the [edit interfaces so-fpc/pic/port sonet-options aps] hierarchy level.

Default  annex-b

Options  annex-a—Use for North American SHDSL network implementations.
annex-b—Use for European SHDSL network implementations.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
apply-action-profile

Syntax  apply-action-profile profile-name;

Hierarchy Level  [edit protocols oam ethernet link-fault-management interface]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Apply the specified action profile to the interface for link-fault management.

Required Privilege Level  interface—To view this statement in the configuration.

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

Related Documentation  • Applying an Action Profile
**aps**

**Syntax**
```plaintext
aps {
    advertise-interval milliseconds;
    annex-b
    authentication-key key;
    (break-before-make | no-break-before-make);
    fast-aps-switch;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    preserve-interface;
    protect-circuit group-name;
    request;
    revert-time seconds;
    switching-mode (bidirectional | unidirectional);
    working-circuit group-name;
}
```

**Hierarchy Level**
[edit interfaces interface-name sonet-options]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Configure Automatic Protection Switching (APS) on the router.

For DS3 channels on a channelized OC12 interface, configure APS on channel 0 only. If you configure APS on channels 1 through 11, it is ignored.

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**
- *Automatic Protection Switching and Multiplex Section Protection Overview*
**arp (Interfaces)**

**Syntax**

```
arp ip-address (mac | multicast-mac) mac-address publish;
```

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

**Syntax (EX Series)**

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

**Hierarchy Level**

```
[edit system]
```

```
[edit interfaces interface-name unit logical-unit-number family inet address address],
```

```
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address]
```

**NOTE:** The edit logical-systems hierarchy is not available on QFabric systems.

**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**

For Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, configure Address Resolution Protocol (ARP) table entries by mapping IP addresses to MAC addresses. You can enable backup VRRP routers to learn ARP requests for VRRP-IP to VRRP-MAC address translation. You can also set the time interval between ARP updates.

**NOTE:** By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the family inet statement. By including the arp statement at the [edit interfaces interface-name unit
logical-unit-number family inet policer] hierarchy level, you can apply a specific ARP-packet policer to an interface. This feature is not available on EX Series switches.

When you need to conserve IP addresses, you can configure an Ethernet interface to be unnumbered by including the unnumbered-address statement at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level.

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

**ip-address**—IP address to map to the MAC address. The IP address specified must be part of the subnet defined in the enclosing **address** statement.

**mac mac-address**—MAC address to map to the IP address. Specify the MAC address as six hexadecimal bytes in one of the following formats: `nnnn.nnnn.nnnn` or `nnn.nnnn.nnnn`. For example, `0000.5e00.5355` or `00:00:5e:00:53:55`.

**multicast-mac mac-address**—Multicast MAC address to map to the IP address. Specify the multicast MAC address as six hexadecimal bytes in one of the following formats: `nnnn.nnnn.nnnn` or `nnn.nnnn.nnnn`. For example, `0000.5e00.5355` or `00:00:5e:00:53:55`.

**publish**—(Optional) Have the router or switch reply to ARP requests for the specified IP address. If you omit this option, the router or switch uses the entry to reach the destination but does not reply to ARP requests.

---

**NOTE:** For unicast MAC addresses only, if you include the **publish** option, the router or switch replies to proxy ARP requests.

---

**aging-timer**—Time interval in minutes between ARP updates. In environments where the number of ARP entries to update is high (for example, on routers only, metro Ethernet environments), increasing the time between updates can improve system performance.

**gratuitous-arp-delay**—(T Series only) Configure a delay for gratuitous ARP requests at the system level. By default, Junos OS sends gratuitous ARP requests immediately after network-related configuration changes are made on an interface (for example, a VLAN ID, MAC address, or IP address change). This might lead to the Packet Forwarding Engine dropping some initial request packets if the configuration updates have not been fully processed. To avoid such request packets being dropped, you can configure a delay in gratuitous ARP requests.

**Values:**

- **seconds**—Configure the ARP request delay in seconds. We recommend configuring a value in the range of 3 through 6 seconds.

**gratuitous-arp-on-ifup**—(ACX Series, SRX Series, T Series only) Add this statement to the [edit system arp] hierarchy to configure Junos OS to automatically issue a gratuitous ARP announcement when an interface is online.

**interfaces**—(T Series only) Specify the ARP aging timer in minutes for a logical interface of family type **inet**.

**Values:**

- **aging-timer minutes**—Time between ARP updates, in minutes.
- **Default:** 20
- **Range:** 1 through 6,00,000
passive-learning—(M Series, MX Series, PTX Series, SRX Series, T Series only) Configure backup VRRP routers or switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests. By default, the backup VRRP router drops these requests; therefore, if the master router fails, the backup router must learn all entries present in the ARP cache of the master router. Configuring passive learning reduces transition delay when the backup router is activated. Learning of ARP mappings (IP-to-MAC address) by backup VRRP routers or switches for hosts sending the requests is disabled unless this statement is configured.

purging—(M Series, MX Series, PTX Series, SRX Series, T Series only) Purge obsolete ARP entries from the cache when an interface or link goes offline.

Required Privilege Level

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

Related Documentation

- Configuring Static ARP Table Entries For Mapping IP Addresses to MAC Addresses
- Configuring Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses
- Junos OS Network Interfaces Library for Routing Devices
- Junos OS System Basics Configuration Guide
- Adjusting the ARP Aging Timer
asynchronous-notification

Syntax

(asynchronous-notification | no-asynchronous-notification);

Hierarchy Level

[edit interfaces ge-fpc/pic/port gigether-options ]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description

(MX Series routers, T Series routers) For all Gigabit Ethernet interfaces (1-Gigabit, 10-Gigabit, and 100-Gigabit), configure support for notification of link down alarm generation and transfer.

(M120 and M320 routers) For all 10-Gigabit Ethernet PIC interfaces, configure support for notification of link down alarm generation and transfer.

- asynchronous-notification—Support notification of link down alarm generation and transfer.
- no-asynchronous-notification—Prohibit notification of link down alarm generation and transfer.

Default

Support for notification of link down alarm generation and transfer is not enabled.

Required Privilege

Level

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

Related Documentation

- Gigabit Ethernet Notification of Link Down Alarm Overview
- Configuring Gigabit Ethernet Notification of Link Down Alarm
atm-encapsulation

Syntax atm-encapsulation (direct | plcp);

Hierarchy Level [edit interfaces at-fpc/pic/port e3-options], [edit interfaces at-fpc/pic/port t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure encapsulation for E3 and T3 traffic over ATM interfaces.

Default Physical Layer Convergence Protocol (PLCP) encapsulation is the default for T3 traffic and for E3 traffic using G.751 framing.

Options
direct—Use direct encapsulation. G.832 framing on E3 interfaces requires direct encapsulation.

plcp—Use PLCP encapsulation.

Required Privilege Level

Required Privilege Level interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

Related Documentation
• Configuring E3 and T3 Parameters on ATM Interfaces
• encapsulation on page 571
atm-options

Syntax

```plaintext
atm-options {
  cell-bundle-size cells;
  ilmi;
  linear-red-profiles profile-name {
    high-plp-max-threshold percent;
    low-plp-max-threshold percent;
    queue-depth cells high-plp-threshold percent low-plp-threshold percent;
  }
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  pic-type (atm1 | atm2);
  plp-to-clp;
  promiscuous-mode {
    vpi vpi-identifier;
  }
  scheduler-maps map-name {
    forwarding-class class-name {
      epd-threshold cells pipi cells;
      linear-red-profile profile-name;
      priority (high | low);
      transmit-weight (cells number | percent number);
    }
    vc-cos-mode (alternate | strict);
  }
  use-null-cw;
  vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
      queue-length number;
    }
  }
}
```

Hierarchy Level

[edit interfaces interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description

Configure ATM-specific physical interface properties.
The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

**NOTE:** Certain options apply only to specific platforms.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface—To view this statement in the configuration.</td>
<td></td>
</tr>
<tr>
<td>interface-control—To add this statement to the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**

- Interface Encapsulations Overview on page 31
- multipoint-destination on page 807
- shaping on page 994
- vci on page 1115

---

**atm-scheduler-map**

**Syntax**

```text
atm-scheduler-map (map-name | default);
```

**Hierarchy Level**

- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Associate a scheduler map with a virtual circuit on a logical interface.

**Options**

- `map-name`—Name of scheduler map that you define at the [edit interfaces interface-name atm-optionsscheduler-maps] hierarchy level.
- `default`—The default scheduler mapping.

**Required Privilege Level**

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

**Related Documentation**

- ATM2 IQ VC Tunnel CoS Components Overview
- scheduler-maps (For ATM2 IQ Interfaces) on page 979
**authentication**

Syntax

```plaintext
authentication [ 
  packet-types [packet-types];
  password password-string;
  username-include [ 
    circuit-id;
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name;
    mac-address;
    option-18;
    option-37;
    option-62 <circuit-id> <remote-id>;
    radius-realm radius-realm-string;
    remote-id;
    user-prefix user-prefix-string;
    vlan-tags;
  ]
]
```

Hierarchy Level

[edit interfaces interface-name auto-configure vlan-ranges],
[edit interfaces interface-name auto-configure stacked-vlan-ranges]

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Specify the authentication parameters that trigger the Access-Request message to AAA for the interface.

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

- Subscribers over Static Interfaces Configuration Overview
- Configuring the Static Subscriber Global Authentication Password
- Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs
- Layer 2 Wholesale with ANCP-Triggered VLANs Overview
**authentication-key**

**Syntax**

```plaintext
authentication-key key;
```

**Hierarchy Level**

[edit interfaces interface-name sonet-options aps]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure the Automatic Protection Switching (APS) authentication key (password).

**Options**

- `key`—Authentication password. It can be 1 through 8 characters long. Configure the same key for both the working and protect routers.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Basic Automatic Protect Switching
- For information about the `authentication-key` statement at the [edit interfaces interface-name unit unit-number family inet address address (vrrp-group | vrrp-inet6-group) group-number] or [edit logical-systems logical-system-name interfaces interface-name unit unit-number family (inet | inet6) address address (vrrp-group | vrrp-inet6-group) group-number] hierarchy level, see the High Availability Feature Guide.

**authentication-profile-name**

**Syntax**

```plaintext
authentication-profile-name access-profile-name;
```

**Hierarchy Level**

[edit protocols dot1x authenticator]

**Release Information**

Statement introduced in Junos OS Release 9.3.

**Description**

Specify the RADIUS authentication profile to use for user authentication when establishing an IEEE 802.1x Port-Based Network Access Control (dot1x) connection.

**Required Privilege Level**

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

**Related Documentation**

- IEEE 802.1x Port-Based Network Access Control Overview
- authenticator on page 434
- dot1x on page 534
authenticator

Syntax

authenticator {
    authentication-profile-name access-profile-name;
    interface interface-id {
        maximum-requests integer;
        quiet-period seconds;
        reauthentication (disable | interval seconds);
        retries integer;
        server-timeout seconds;
        supplicant (single);
        supplicant-timeout seconds;
        transmit-period seconds;
    }
}

Hierarchy Level
[edit protocols dot1x]

Release Information
Statement introduced in Junos OS Release 9.3.

Description
Specify an authentication profile for user or client authentication and configure the Ethernet interface for 802.1x protocol operation.

Options

- **authentication-profile-name access-profile-name**—Specifies the RADIUS authentication profile for user or client authentication.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- IEEE 802.1x Port-Based Network Access Control Overview
- authentication-profile-name on page 433
- dot1x on page 534
auto-configure

Syntax

```
auto-configure {
    vlan-ranges {
        access-profile profile-name;
        authentication {
            packet-types [packet-types];
            password password-string;
            username-password {
                circuit-id;
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                mac-address;
                option-18;
                option-37;
                option-82 <circuit-id> <remote-id>;
                radius-realm radius-realm-string;
                remote-id;
                user-prefix user-prefix-string;
                vlan-tags;
            }
        }
        dynamic-profile profile-name {
            accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
            ranges (any | low-tag–high-tag), (any | low-tag–high-tag);
        }
        override;
    }
    stacked-vlan-ranges {
        access-profile profile-name;
        authentication {
            packet-types [packet-types];
            password password-string;
            username-password {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                mac-address;
                option-18;
                option-37;
                option-82 <circuit-id> <remote-id>;
                radius-realm radius-realm-string;
                remote-id;
                user-prefix user-prefix-string;
                vlan-tags;
            }
        }
        dynamic-profile profile-name {
            accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
            ranges (any | low-tag–high-tag), (any | low-tag–high-tag);
        }
```

Copyright © 2019, Juniper Networks, Inc.
auto-discovery

Syntax

auto-discovery;

Hierarchy Level [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]

Release Information Statement introduced in Junos OS Release 8.4.

Description Enable the MEP to accept continuity check messages from all remote MEPs.

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

Related Documentation

• Configuring a MEP to Generate and Respond to CFM Protocol Messages
auto-negotiation

Syntax
(auto-negotiation | no-auto-negotiation) <remote-fault (local-interface-online | local-interface-offline)>;

Hierarchy Level
[edit interfaces interface-name ether-options],
[edit interfaces interface-name gighether-options],
[edit interfaces ge-pim/0/0 switch-options switch-port port-number]

Release Information
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description
For Gigabit Ethernet interfaces on M Series, MX Series, T Series, TX Matrix routers, and ACX Series routers explicitly enable autonegotiation and remote fault. For EX Series switches, explicitly enable autonegotiation only.

- **auto-negotiation**—Enables autonegotiation. This is the default.
- **no-auto-negotiation**—Disable autonegotiation. When autonegotiation is disabled, you must explicitly configure the link mode and speed.

When you configure Tri-Rate Ethernet copper interfaces to operate at 1 Gbps, autonegotiation must be enabled.

NOTE: On EX Series switches, an interface configuration that disables autonegotiation and manually sets the link speed to 1 Gbps is accepted when you commit the configuration; however, if the interface you are configuring is a Tri-Rate Ethernet copper interface, the configuration is ignored as invalid and autonegotiation is enabled by default.

To correct the invalid configuration and disable autonegotiation:
1. Delete the no-auto-negotiation statement and commit the configuration.
2. Set the link speed to 10 or 100 Mbps, set no-auto-negotiation, and commit the configuration.

On EX Series switches, if the link speed and duplex mode are also configured, the interfaces use the values configured as the desired values in the negotiation. If autonegotiation is disabled, the link speed and link mode must be configured.

NOTE: On T4000 routers, the auto-negotiation command is ignored for interfaces other than Gigabit Ethernet.
NOTE: On ACX Series routers, when you configure fiber interfaces (fiber media mode) to operate at 1 Gbps, autonegotiation is enabled by default to negotiate the speed and duplex settings. You can disable autonegotiation by using the (no-auto-negotiation) statement, and commit the configuration. In the fiber media mode. In copper interfaces (copper media mode), autonegotiation is enabled by default. To disable autonegotiation, you need to explicitly configure the link speed to 10 or 100 Mbps, set no-auto-negotiation, and commit the configuration.

**Default**

Autonegotiation is automatically enabled. No explicit action is taken after the autonegotiation is complete or if the negotiation fails.

**Options**

remote-fault (local-interface-online | local-interface-offline)—(Optional) For M Series, MX Series, T Series, TX Matrix routers, and ACX Series routers only, manually configure remote fault on an interface.

Default: local-interface-online

**Required Privilege Level**

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

**Related Documentation**

- Gigabit Ethernet Autonegotiation Overview
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support
backup-destination

Syntax
backup-destination address;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For tunnel interfaces, specify the remote address of the backup tunnel.

Options
address—Address of the remote side of the connection.

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

Related Documentation
- Junos OS Services Interfaces Library for Routing Devices
- destination (Tunnels) on page 520

backup-interface

Syntax
backup-interface es-fpc/pic/port;

Hierarchy Level
[edit interfaces es-fpc/pic/port es-options]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure a backup ES Physical Interface Card (PIC). If the primary ES PIC fails, the backup becomes active, inherits all the tunnels and security associations (SAs), and acts as the new next hop for IP Security (IPsec) traffic.

Options
es-fpc/pic/port—Name of ES interface to serve as the backup.

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

Related Documentation
- Junos OS Services Interfaces Library for Routing Devices
backup-options

Syntax
backup-options { interface interface-name; }

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure an interface to be used as a backup interface if the primary interface goes down. This is used to support ISDN dial backup operation.

The remaining statement is 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
• Junos OS Interfaces and Routing Configuration Guide
bandwidth (Interfaces)

Syntax

bandwidth rate;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

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 bandwidth value for an interface. This statement is valid for all logical interface types except multilink and aggregated interfaces.

NOTE: We recommend that you be careful when setting this value. Any interface bandwidth value that you configure using the bandwidth statement affects how the interface cost is calculated for a dynamic routing protocol, such as OSPF. By default, the interface cost for a dynamic routing protocol is calculated using the following formula:

\[ \text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}}, \]

where bandwidth is the physical interface speed. However, if you specify a value for bandwidth using the bandwidth statement, that value is used to calculate the interface cost, rather than the actual physical interface bandwidth.

Options

rate—Peak rate, in bits per second (bps) or cells per second (cps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

Range: Not limited.

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 Bandwidth on page 173
bandwidth-limit (Hierarchical Policer)

Syntax

```
bandwidth-limit bps;
```

Hierarchy Level

```
[edit dynamic-profiles profile-name firewall hierarchical-policer aggregate if-exceeding],
[edit dynamic-profiles profile-name firewall hierarchical-policer premium if-exceeding],
[edit firewall hierarchical-policer aggregate if-exceeding],
[edit firewall hierarchical-policer premium if-exceeding]
```

Release Information

Statement introduced in Junos OS Release 9.5. Support at the **[edit dynamic-profiles ... if-exceeding]** hierarchy level introduced in Junos OS Release 11.4.

Description

On M40e, M120, and M320 (with FFPC and SFPC) edge routers; on MPCs hosted on MX Series routers; on T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs; and on T4000 routers with Type 5 FPC and Enhanced Scaling Type 4 FPC, configure the maximum average bandwidth for premium or aggregate traffic in a hierarchical policer.

Options

**bps**—You can specify the number of bits per second either as a decimal number or as a decimal number followed by the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range:

- 32,000 through 50,000,000,000 on M Series routers
- 32,000 through 100,000,000,000 on T Series routers
- 32,000 through 18,446,744,073,709,551,615 on MX Series routers

**NOTE:** When you specify a numeric value beyond the supported bandwidth of the PFE, the router caps the bandwidth at the maximum supported bandwidth of the PFE.

Required Privilege Level

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

Related Documentation

- *Hierarchical Policer Configuration Overview*
- *Policer Bandwidth and Burst-Size Limits*
- *Policer Color-Marking and Actions*
- *Single Token Bucket Algorithm*
- *Determining Proper Burst Size for Traffic Policers*
- aggregate (Hierarchical Policer)
- burst-size-limit (Hierarchical Policer) on page 455
- premium (Hierarchical Policer) on page 918

**bandwidth-limit (Policer for Gigabit Ethernet Interfaces)**

**Syntax**

```
bandwidth-limit bps;
```

**Hierarchy Level**

```
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name aggregate],
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name premium]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Define a policer to apply to nonpremium traffic.

**Options**

**bps**—Bandwidth limit, in bits per second. Specify either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

**Range:** 32 kbps through 32 gigabits per second (Gbps). For IQ2 and IQ2-E interfaces 65,536 bps through 1 Gbps. For 10-Gigabit IQ2 and IQ2-E interfaces 65,536 bps through 10 Gbps.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Gigabit Ethernet Policers
- burst-size-limit (Policer for Gigabit Ethernet Interfaces) on page 456
**bearer-bandwidth-limit**

**Syntax**  
`bearer-bandwidth-limit kilobits-per-second;`

**Hierarchy Level**  
- `[edit interfaces interface-name unit logical-unit-number dynamic-call-admission-control]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number dynamic-call-admission-control]`

**Release Information**  
Statement introduced in Junos OS Release 8.2.

**Description**  
(J4350 and J6350 Services Routers supporting voice over IP with the TGM550 media gateway module) For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure the bearer bandwidth limit (BBL). BBL is used for dynamic call admission control (dynamic CAC) to provide enhanced control over WAN bandwidth.

**Options**  
`kilobits-per-second`—The bearer bandwidth limit to be reported to a TGM550 media gateway module, in kilobits per second (kbps).

- **Range:** 0 through 9999 kbps
- **Default:** 1 (dynamic CAC is not enabled on the interface)

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

**Related Documentation**  
- Junos OS Services Interfaces Library for Routing Devices
- Junos OS Interfaces and Routing Configuration Guide
bert-algorithm

**Syntax**

```
bert-algorithm algorithm;
```

**Hierarchy Level**

[edit interfaces ce1-fpc/pic/port],
[edit interfaces ct1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name el1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**

Configure the pattern to send in the bit stream during a bit error rate test (BERT). Applies to T1, E3, T3, and multichannel DS3 interfaces, the channelized interfaces (DS3, OC12, STM1), and channelized IQ and IQE interfaces (E1, E3 and DS3).

**NOTE:** When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the bert-algorithm statement must be included at the [edit interfaces ce1-fpc/pic/port] or [edit interfaces ct1-fpc/pic/port] hierarchy level as appropriate.

**Options**

`algorithm`—Pattern to send in the bit stream. There are two categories of test patterns: pseudorandom and repetitive. Both patterns conform to CCITT/ITU O.151, O.152, O.153, and O.161 standards. The algorithm can be one of the following patterns:

- `all-ones-repeating`—Pattern is all ones.
- `all-zeros-repeating`—Pattern is all zeros.
- `alternating-double-ones-zeros`—Pattern is alternating pairs of ones and zeros.
- `alternating-ones-zeros`—Pattern is alternating ones and zeros.
- `pseudo-2e3`—Pattern is $2^3 - 1$.
- `pseudo-2e4`—Pattern is $2^4 - 1$.
- `pseudo-2e5`—Pattern is $2^5 - 1$.
- `pseudo-2e6`—Pattern is $2^6 - 1$.
- `pseudo-2e7`—Pattern is $2^7 - 1$.
- `pseudo-2e9-o153`—Pattern is $2^9 - 1$, as defined in the O153 standard.
- `pseudo-2e10`—Pattern is $2^{10} - 1$. 
• pseudo-2e11-o152—Pattern is $2^{11} - 1$, as defined in the O152 standard.
• pseudo-2e15-o151—Pattern is $2^{15} - 1$, as defined in the O151 standard.
• pseudo-2e17—Pattern is $2^{17} - 1$.
• pseudo-2e18—Pattern is $2^{18} - 1$.
• pseudo-2e20-o151—Pattern is $2^{20} - 1$, as defined in the O151 standard.
• pseudo-2e20-o153—Pattern is $2^{20} - 1$, as defined in the O153 standard.
• pseudo-2e21—Pattern is $2^{21} - 1$.
• pseudo-2e22—Pattern is $2^{22} - 1$.
• pseudo-2e23-o151—Pattern is $2^{23} - 1$, as defined in the O151 standard.
• pseudo-2e25—Pattern is $2^{25} - 1$.
• pseudo-2e28—Pattern is $2^{28} - 1$.
• pseudo-2e29—Pattern is $2^{29} - 1$.
• pseudo-2e31—Pattern is $2^{31} - 1$.
• pseudo-2e32—Pattern is $2^{32} - 1$.
• repeating-1-in-4—One bit in four is set to 1; the others are set to 0.
• repeating-1-in-8—One bit in eight is set to 1; the others are set to 0.
• repeating-3-in-24—Three bits in twenty four are set to 1; the others are set to 0.

Default: pseudo-2e3

Related Documentation

- Interface Diagnostics
- Configuring E1 BERT Properties
- Configuring E3 BERT Properties
- Configuring T1 BERT Properties
- Configuring T3 BERT Properties
- Examples: Configuring T3 Interfaces
- bert-error-rate on page 447
- bert-period on page 449

Required Privilege

Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
**bert-error-rate**

**Syntax**

```
bert-error-rate rate;
```

**Hierarchy Level**

```
[edit interfaces ce1-fpc/pic/port],
[edit interfaces ct1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name el1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]
```

**Release Information**


**Description**

Configure the bit error rate to use in a BERT procedure. Applies to E1, E3, T1, or T3 interfaces, and to the channelized interfaces (DS3, OC3, OC12, and STM1).

---

**NOTE:** When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the bert-error-rate statement must be included at the [edit interfaces ce1-fpc/pic/port] or [edit interfaces ct1-fpc/pic/port] hierarchy level as appropriate.

---

**Options**

- **rate**—Bit error rate.
  - **Range:** 0 through 7, which corresponds to $10^{-1}$ (1 error per bit) to $10^{-7}$ (1 error per 10 million bits)
  - **Default:** 0

**Required Privilege Level**

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

**Related Documentation**

- bert-algorithm on page 445
- bert-period on page 449
- ds0-options on page 538
- e1-options on page 562
- e3-options on page 563
- t1-options on page 1037
- t3-options on page 1041
- Interface Diagnostics
• Configuring E1 BERT Properties
• Configuring E3 BERT Properties
• Configuring T1 BERT Properties
• Configuring T3 BERT Properties
• Examples: Configuring T3 Interfaces
bert-period

Syntax  
bert-period seconds;

Hierarchy Level  
[edit interfaces ce1-fpc/pic/port],  
[edit interfaces ct1-fpc/pic/port],  
[edit interfaces interface-name ds0-options],  
[edit interfaces interface-name el-options],  
[edit interfaces interface-name e3-options],  
[edit interfaces interface-name t1-options],  
[edit interfaces interface-name t3-options]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description  
Configure the duration of a BERT test. Applies to E1, E3, T1, and T3 interfaces, and to E1, E3, T1, and T3 partitions on the channelized interfaces (CE1, CT1, DS3, OC3, OC12, OC48, STM1, STM4, and STM16).

E1 and T1 IQ, IQE, and standard interfaces support an extended BERT period range, up to 86,400 seconds (24 hours).

NOTE: When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the bert-period statement must be included at the [edit interfaces ce1-fpc/pic/port] or [edit interfaces ct1-fpc/pic/port] hierarchy level as appropriate.

Options  
seconds—Test duration. Range and default values vary by interface type.  
Range:

- PIC-dependent—Normal BERT period: either 1 through 239 seconds or 1 through 240 seconds
- PIC-dependent—Extended BERT period: from 1 through 86,400 seconds

Default:

- Normal BERT period: 10 seconds
- Extended BERT period (on supported E1 interfaces): 10 seconds
- Extended BERT period (on supported T1 interfaces): 240 seconds

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

- Interface Diagnostics
- Configuring E1 BERT Properties
- Configuring E3 BERT Properties
- Configuring T1 BERT Properties
- Configuring T3 BERT Properties
- bert-algorithm on page 445
- bert-error-rate on page 447

bridge-domain

Syntax

```
bridge-domain name;
    vlan-id [ vlan-identifiers ];
}
```

Hierarchy Level

- [edit protocols oam ethernet connectivity-fault-management maintenance-domain maintenance-domain-name]
- [edit protocols oam ethernet connectivity-fault-management maintenance-domain maintenance-domain-name virtual-switch virtual-switch-name]

Release Information

Statement introduced in Junos OS Release 9.4.

Description

(MX Series routers only) Specify the OAM Ethernet CFM maintenance domain bridge domain.

Options

- **name**—Specify the name of the bridge domain.
- **vlan-identifiers**—Specify one or more VLAN identifiers.

Required Privilege Level

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

Related Documentation

- Configuring Maintenance Intermediate Points (MIPs)
- maintenance-domain on page 777
broadcast

Syntax broadcast address;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family family address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address 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 Set the broadcast address on the network or subnet. On a subnet you cannot specify a host address of 0 (0.0.0.0), nor can you specify a broadcast address (255.255.255.255). For example, in the statement set interface ge-0/0/0 unit 0 family inet address 10.1.1.0/24, the subnet address 10.1.1.0 has the host address of 0. Hence, you cannot configure this address. Similarly, for the subnet, you cannot use the broadcast address 10.1.1.255/24.

Default The default broadcast address has a host portion of all ones.

Options address—Broadcast address. The address must have a host portion of either all ones or all zeros. You cannot specify the addresses 0.0.0.0 or 255.255.255.255.

NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

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 Address on page 191
**buildout (E3 or T3 over ATM Interfaces)**

Syntax  
buildout feet;

Hierarchy Level  
[edit interfaces at-fpc/pic/port e3-options],  
[edit interfaces at-fpc/pic/port t3-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For E3 and T3 traffic over ATM interfaces, set the buildout value.

Options  
**feet**—The buildout value in feet.  
**Range:** 0 through 450 feet (137 meters)  
**Default:** 10 feet (3 meters)

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

Related Documentation  
- Configuring E3 and T3 Parameters on ATM Interfaces
**buildout (T1 Interfaces)**

**Syntax**

buildout value;

**Hierarchy Level**

[edit interfaces ct1-fpc/pic/port]
[edit interfaces interface-name t1-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**

For T1 interfaces, set the buildout value.

**NOTE:** When configuring CT1 interfaces on 10-port Channelized E1/T1 IQE PICs and 16-Port Channelized E1/T1 Circuit Emulation MICs, the buildout statement must be included at the hierarchy level.

**Default**

The default buildout value is 0 through 132 feet.

**Options**

You can set the buildout value to one of the following:

- 0-132—0 through 132 feet (0 through 40 meters)
- 133-265—133 through 265 feet (40 through 81 meters)
- 266-398—266 through 398 feet (81 through 121 meters)
- 399-531—399 through 531 feet (121 through 162 meters)
- 532-655—532 through 655 feet (162 through 200 meters)
- **long-7.5db**—For MX Series only, long buildout with 7.5 dB transmit attenuation
- **long-15db**—For MX Series only, long buildout with 15 dB transmit attenuation
- **long-22.5db**—For MX Series only, long buildout with 22.5 dB transmit attenuation

**Required Privilege Level**

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

**Related Documentation**

- Configuring the T1 Buildout
- Junos OS Interfaces and Routing Configuration Guide
bundle

Syntax

bundle (ml-fpc/pic/port | ls-fpc/pic/port);

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Associate the multilink interface with the logical interface it is joining. You can include this statement for the mlfr-end-to-end and mlfr-uni-nni protocol families only.

NOTE:

For M Series routers and T Series routers, the following caveats apply:

- Maximum supported throughput on the bundle interfaces is 45 Mbps.
- Bundling of the logical interfaces under a T3 physical interface into the same or different bundles is not supported.

Options

ml-fpc/pic/port—Name of the multilink interface you are linking.

ls-fpc/pic/port—Name of the link services interface you are linking.

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

- Junos OS Services Interfaces Library for Routing Devices
burst-size-limit (Hierarchical Policer)

Syntax

burst-size-limit bytes;

Hierarchy Level

[edit dynamic-profiles profile-name firewall hierarchical-policer aggregate if-exceeding],
[edit dynamic-profiles profile-name firewall hierarchical-policer premium if-exceeding],
[edit firewall hierarchical-policer aggregate if-exceeding],
[edit firewall hierarchical-policer premium if-exceeding]

Release Information

Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles ... if exceeding] hierarchy level introduced in Junos OS Release 11.4.

Description

On M40e, M120, and M320 (with FFPC and SFPC) edge routers; on MPCs hosted on MX Series routers; on T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs; and on T4000 routers with Type 5 FPC and Enhanced Scaling Type 4 FPC, configure the burst-size limit for premium or aggregate traffic in a hierarchical policer.

Options

bytes—Burst-size limit in bytes. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed. You can specify the value either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

Range: 1500 through 2,147,450,880 (1500 through 100,000,000,000 on MPCs hosted on MX Series routers)

Required Privilege

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

Related Documentation

- Hierarchical Policer Configuration Overview
- Policer Bandwidth and Burst-Size Limits
- Policer Color-Marking and Actions
- Single Token Bucket Algorithm
- Determining Proper Burst Size for Traffic Policers
- Hierarchical Policers
- aggregate (Hierarchical Policer)
- bandwidth-limit (Hierarchical Policer) on page 442
- premium (Hierarchical Policer) on page 918
burst-size-limit (Policer for Gigabit Ethernet Interfaces)

Syntax
burst-size-limit bytes;

Hierarchy Level
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name aggregate],
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name premium]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define a policer to apply to nonpremium traffic.

Options
bytes—Burst length.
Range: 1500 through 100,000,000 bytes

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

Related Documentation
• Configuring Gigabit Ethernet Policers
• bandwidth-limit (Policer for Gigabit Ethernet Interfaces) on page 443
**byte-encoding**

Syntax: byte-encoding (nx56 | nx64);

Hierarchy Level: [edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name t1-options]

Release Information: Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description: Set the byte encoding on a DS0 or T1 interface to use 7 bits per byte or 8 bits per byte.

**NOTE:** When configuring T1 interfaces on the 10-port Channelized E1/T1 IQE PIC, the byte-encoding statement must be included at the [edit interfaces t1-fpc/pic/port] hierarchy level.

Default: The default byte encoding is 8 bits per byte (nx64).

Options: nx56—Use 7 bits per byte.

nx64—Use 8 bits per byte.

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

Related Documentation: Configuring T1 Byte Encoding

Copyright © 2019, Juniper Networks, Inc. 457
**bytes**

**Syntax**
```
bytes {
  c2 value;
  e1-quiet value;
  f1 value;
  f2 value;
  s1 value;
  z3 value;
  z4 value;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name sonet-options]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Set values in some SONET/SDH header bytes.

**Options**

- **c2 value**—Path signal label SONET/SDH overhead byte. SONET/SDH frames use the C2 byte to indicate the contents of the payload inside the frame. SONET/SDH interfaces use the C2 byte to indicate whether the payload is scrambled.
  
  **Range:** 0 through 255
  
  **Default:** 0xCF

- **e1-quiet value**—Default idle byte sent on the orderwire SONET/SDH overhead bytes. The router does not support the orderwire channel, and hence sends this byte continuously.
  
  **Range:** 0 through 255
  
  **Default:** 0x7F

- **f1 value, f2 value, z3 value, z4 value**—SONET/SDH overhead bytes.
  
  **Range:** 0 through 255
  
  **Default:** 0x00

- **s1 value**—Synchronization message SONET overhead byte. This byte is normally controlled as a side effect of the system reference clock configuration and the state of the external clock coming from an interface if the system reference clocks have been configured to use an external reference.
  
  **Range:** 0 through 255
  
  **Default:** 0xCC

**Required Privilege**
- **Level** interface—To view this statement in the configuration.
- **Level** interface-control—To add this statement to the configuration.
calculation-weight

Syntax

```
calculation-weight {
  delay delay-value;
  delay-variation delay-variation-value;
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.1.
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description

Configure the calculation weight for delay and delay variation.

NOTE: This option is applicable only for two-way delay measurement.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation

- Configuring an Iterator Profile
- Configuring an Iterator Profile on a Switch (CLI Procedure)
- delay
- delay-variation
### callback

**Syntax**
```
callback;
```

**Hierarchy Level**
```
[edit interfaces dl unit logical-unit-number dialer-options incoming-map],
[edit logical-systems logical-system-name interfaces dl unit logical-unit-number dialer-options incoming-map]
```

**Release Information**
Statement introduced in Junos OS Release 7.5.

**Description**
On J Series Services Routers with interfaces configured for ISDN, configure the dialer to terminate the incoming call and call back the originator after the callback wait period. The default wait time is 5 seconds. To configure the wait time, include the `callback-wait-period` statement at the `[edit interfaces dl unit logical-unit-number dialer-options]` hierarchy level.

**NOTE:** The incoming-map statement is mandatory for the router to accept any incoming ISDN calls.

If the `callback` statement is configured, you cannot use the `caller caller-id` statement at the `[edit interfaces dl unit logical-unit-number dialer-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**
- Junos OS Interfaces and Routing Configuration Guide
- `callback-wait-period` on page 461
callback-wait-period

**Syntax**

callback-wait-period time;

**Hierarchy Level**

[edit interfaces dl unit logical-unit-number dialer-options],
[edit logical-systems logical-system-name interfaces dl unit logical-unit-number dialer-options]

**Release Information**

Statement introduced in Junos OS Release 7.5.

**Description**

On J Series Services Routers with interfaces configured for ISDN with callback, specify the amount of time the dialer waits before calling back the caller. The default wait time is 5 seconds. The wait time is necessary because, when a call is rejected, the switch waits for up to 4 seconds on point-to-multipoint connections to ensure no other device accepts the call before sending the DISCONNECT message to the originator of the call. However, the default time of 5 seconds may not be sufficient for different switches or may not be needed on point-to-point connections.

To configure callback mode, include the callback statement at the [edit interfaces dl unit logical-unit-number dialer-options] hierarchy level.

If the callback statement is configured, you cannot use the caller caller-id statement at the [edit interfaces dl unit logical-unit-number dialer-options] hierarchy level.

**Options**

- **time**—Time the dialer waits before calling back the caller.

**Required Privilege Level**

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

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide
**caller**

**Syntax**  
caller (caller-id | accept-all);

**Hierarchy Level**  
[edit interfaces dln unit logical-unit-number dialer-options incoming-map],  
[edit logical-systems logical-system-name interfaces dln unit logical-unit-number dialer-options incoming-map]

**Release Information**  
Statement introduced in Junos OS Release 7.5.

**Description**  
On J Series Services Routers with interfaces configured for ISDN, specify the dialer to accept a specified caller number or accept all incoming calls.

**Options**  
**caller-id**—Incoming caller number. You can configure multiple caller IDs on a dialer. The caller ID of the incoming call is matched against all caller IDs configured on all dialers. The dialer matching the caller ID is looked at for further processing. Only a precise match is a valid match. For example, the configured caller ID 1-222-333-4444 or 222-333-4444 will match the incoming caller ID 1-222-333-4444.

If the incoming caller ID has fewer digits than the number configured, it is not a valid match. Duplicate caller IDs are not allowed on different dialers; however, for example, the numbers 1-408-532-1091, 408-532-1091, and 532-1091 can still be configured on different dialers.

Only one B-channel can map to one dialer. If one dialer is already mapped, any other call mapping to the same dialer is rejected (except in the case of a multilink dialer). If no dialer caller is configured on a dialer, that dialer will not accept any calls.

**accept-all**—Any incoming call in an associated interface is accepted.

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

**Related Documentation**  
* Junos OS Interfaces and Routing Configuration Guide
calling-number

Syntax

\[
\text{calling-number number;}
\]

Hierarchy Level

[edit interfaces br-pim/0/port isdn-options]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

On J Series Services Routers with ISDN interfaces, configure the calling number to include in outgoing calls.

Options

\[\text{number—Calling number.}\]

Required Privilege

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring ISDN Physical Interface Properties

• Junos OS Interfaces and Routing Configuration Guide
### cbit-parity

**Syntax**
\[(cbit-parity | no-cbit-parity);\]

**Hierarchy Level**
\[edit interfaces interface-name t3-options\]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For T3 interfaces only, enable or disable C-bit parity mode, which controls the type of framing that is present on the transmitted T3 signal. When C-bit parity mode is enabled, the C-bit positions are used for the far-end block error (FEBE), far-end alarm and control (FEAC), terminal data link, path parity, and mode indicator bits, as defined in ANSI T1.107a-1989. For ATM and ATM2 IQ2 and IQ2-E interfaces, M23 framing is used when the `no-cbit-parity` statement is included. For all other interfaces, M13 framing is used when the `no-cbit-parity` statement is included.

**Default**
C-bit parity mode is enabled.

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

**Related Documentation**
- [Configuring E3 and T3 Parameters on ATM Interfaces](#)
- [Disabling T3 C-Bit Parity Mode](#)
cbr

**Syntax**
cbr rate;

**Hierarchy Level**
[edit interfaces at-fpc/pic/port atm-options vpi vpi-identifier shaping],
[edit interfaces at-fpc/pic/port unit logical-unit-number address address family family multipoint-destination address shaping],
[edit interfaces at-fpc/pic/port unit logical-unit-number shaping],
[edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number address address family family multipoint-destination address shaping],
[edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number shaping]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For ATM encapsulation only, define a constant bit rate bandwidth utilization in the traffic-shaping profile.

**Default**
Unspecified bit rate (UBR); that is, bandwidth utilization is unlimited.

**Options**
rate—Peak rate, in bits per second (bps) or cells per second (cps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

For ATM1 and ATM2 OC3 interfaces, the maximum available rate is 100 percent of line-rate, or 135,600,000 bps. For ATM1 OC12 interfaces, the maximum available rate is 50 percent of line-rate, or 271,263,396 bps. For ATM2 IQ interfaces, the maximum available rate is 542,526,792 bps.

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

**Related Documentation**
- Defining the ATM Traffic-Shaping Profile Overview
- rtvbr on page 973
- shaping on page 994
- vbr on page 1113
cell-bundle-size

Syntax  

```
cell-bundle-size cells;
```

Hierarchy Level  

[edit interfaces at-fpc/pic/port atm-options],
[edit interfaces at-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number]

Release Information  

Statement introduced before Junos OS Release 7.4.

Description  

For ATM2 IQ interfaces using ATM Layer 2 circuit cell-relay transport mode only, configure the maximum number of ATM cells per frame.

**NOTE:** For MIC-3D-8OC3-2OC12-ATM on MX104 routers, ensure that the configured cell-bundle-size is less than 30 for an ATM interface that is configured with atm-ccc-cell-relay encapsulation. If the configured cell-bundle-size is greater than or equal to 30 and the traffic is passing through the interface at line rate, it might lead to AFEB crash.

Options  

- **cells**—Maximum number of cells.

  Default: 1 cell

  Range: 1 through 176 cells

Required Privilege Level

- interface—to view this statement in the configuration.

- interface-control—to add this statement to the configuration.

Related Documentation  

- Configuring the Layer 2 Circuit Cell-Relay Cell Maximum Overview
chap

Syntax
chap {
    access-profile name;
    challenge-length minimum minimum-length maximum maximum-length;
    default-chap-secret name;
    local-name name;
    passive;
}

Hierarchy Level
[edit interfaces interface-name ppp-options],
[edit interfaces interface-name unit logical-unit-number ppp-options],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Allow each side of a link to challenge its peer, using a “secret” known only to the authenticator and that peer. The secret is not sent over the link.

By default, PPP CHAP is disabled. If CHAP is not explicitly enabled, the interface makes no CHAP challenges and denies all incoming CHAP challenges.

For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over AAL5 LLC encapsulation.
- atm-ppp-vc-mux—PPP over AAL5 multiplex encapsulation.

BEST PRACTICE: On inline service (si) interfaces for L2TP, only the chap statement itself is typically used for subscriber management. We recommend that you leave the subordinate statements at their default values.

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
- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
- Applying PPP Attributes to L2TP LNS Subscribers with a User Group Profile
- Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface
circuit-type

Syntax  
circuit-type;

Hierarchy Level  
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include],

Release Information  
Statement introduced in Junos OS Release 10.0.

Description  
Specify that the circuit type is concatenated with the username during the subscriber authentication process.

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

Related Documentation  
• Configuring VLAN Interface Username Information for AAA Authentication

cisco-interoperability

Syntax  
cisco-interoperability send-lip-remove-link-for-link-reject;

Hierarchy Level  
[edit interfaces interface-name mlfr-uni-nni-bundle-options]

Release Information  
Statement introduced in Junos OS Release 7.4.

Description  
FRF.16 interoperability settings.

Options  
send-lip-remove-link-for-link-reject—Send Link Integrity Protocol remove link when an add-link rejection message is received.

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

Related Documentation  
• Junos OS Services Interfaces Library for Routing Devices
classifier

Syntax

classifier {
  per-unit-scheduler {
    forwarding-class class-name {
      loss-priority (high | low);
    }
  }
}

Hierarchy Level
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the classifier for the output priority map to be applied to outgoing frames on this interface.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
- Specifying an Output Priority Map
- input-priority-map on page 682
clear-dont-fragment-bit

**Syntax**
clear-dont-fragment-bit;

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

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Clear the don't-fragment (DF) bit on all IP version 4 (IPv4) packets entering a generic routing encapsulation (GRE) tunnel. If the encapsulated packet's size exceeds the tunnel's maximum transmission unit (MTU), the packet is fragmented before encapsulation. The statement is supported only on MX Series routers and all M Series routers except the M320 router.

When you configure the `clear-dont-fragment-bit` statement on an interface with the MPLS protocol family enabled, you must specify an MTU value. This MTU value must not be greater than maximum supported value, which is 9192.

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

**Related Documentation**
- Junos OS Services Interfaces Library for Routing Devices
clock-rate

Syntax  clock-rate rate;

Hierarchy Level  [edit interfaces interface-name serial-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For EIA-530 and V.35 interfaces, configure the interface speed, in meghertz (MHz).

Options  rate—You can specify one of the following rates:

- 2.048 MHz
- 2.341 MHz
- 2.731 MHz
- 3.277 MHz
- 4.096 MHz
- 5.461 MHz
- 8.192 MHz
- 16.384 MHz

Default: 16.384 MHz

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

Related Documentation  • Configuring the Serial Clocking Mode on page 322
clocking

Syntax    clocking (external [interface interface-name] | internal);

Hierarchy Level    [edit interfaces interface-name]

Release Information    Statement introduced before Junos OS Release 7.4.
    interface option added in Junos OS Release 8.2.
    Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description    For interfaces that can use various clock sources, configure the source of the transmit clock on each interface.

NOTE: On Channelized SONET/SDH PICs, if you set the parent (or the master) controller clock to external, then you must set the child controller clocks to the default value—that is, internal.

For example, on the Channelized STM1 PIC, if the clock on the Channelized STM1 interface (which is the master controller) is set to external, then you must not configure the CE1 interface (which is the child controller) clock to external. Instead you must configure the CE1 interface clock to internal.

Options    external—The clock source is provided by the data communication equipment (DCE).

    interface interface-name—Configure clocking for the drop-and insert feature. When configuring this feature, both ports must use the same clock source: either the router’s internal clock or an external clock on one of the interfaces. If an external clock source is required, one interface must specify clocking external and the other must specify the same clock.

    internal—Use the internal stratum 3 clock as the reference clock.

Default: internal

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

Related Documentation    • Configuring the Clock Source on page 113
    • Configuring the Clock Source on SONET/SDH Interfaces
    • Clock Sources on Channelized Interfaces
    • Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots
    • loop-timing on page 759
clocking-mode

**Syntax**
clocking-mode (dce | internal | loop);

**Hierarchy Level**
[edit interfaces interface-name serial-options]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For EIA-530 and V.35 interfaces, configure the clock mode. You cannot configure clocking-mode dce on a DTE router using an X.21 serial line protocol (detected automatically when an X.21 cable is plugged into the serial interface).

**Options**
dce—DCE timing (DTE mode only, not valid for X.21).

internal—Internal baud timing.

loop—Loop timing.

Default: loop

**Required Privilege**
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration

**Related Documentation**
- Configuring the Serial Clocking Mode on page 322
community (Policy Options)

Syntax

```
community name [invert-match; members [community-ids];]
```

Hierarchy Level

[edit dynamic policy-options], [edit logical-systems logical-system-name policy-options], [edit policy-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
Support for BGP large community introduced in Junos OS Release 17.3 for MX Series, PTX Series, and QFX Series.

Description

Define a community, extended community or large community for use in a routing policy match condition.

Options

- **name**—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters. To include spaces in the name, enclose it in quotation marks (" ").

- **invert-match**—Invert the results of the community expression matching. The community match condition defines a regular expression and if it matches the community attribute of the received prefix, Junos OS returns a TRUE result. If not, Junos OS returns a FALSE result. The `invert-match` statement makes Junos OS behave to the contrary. If there is a match, Junos OS returns a FALSE result. If there is no match, Junos OS returns a TRUE result.

- **members community-ids**—One or more community members. If you specify more than one member, you must enclose all members in brackets.

The format for `community-ids` is:

```
as-number:community-value
```

Starting in Junos OS Release 15.1, you can apply a wildcard member `segmented-nh::.*:0` to apply the BGP policy to all the S-PMSI A-D routes carrying extended community information.

`as-number` is the AS number and can be a value in the range from 0 through 65,535.

`community-value` is the community identifier and can be a number in the range from 0 through 65,535.
You also can specify **community-ids** for communities as one of the following well-known community names, which are defined in RFC 1997, *BGP Communities Attribute*:

- **no-export**—Routes containing this community name are not advertised outside a BGP confederation boundary.

- **no-advertise**—Routes containing this community name are not advertised to other BGP peers.

- **no-export-subconfed**—Routes containing this community name are not advertised to external BGP peers, including peers in other members' ASs inside a BGP confederation.

You can explicitly exclude BGP community information with a static route using the **none** option. Include **none** when configuring an individual route in the **route** portion of the **static** statement to override a **community** option specified in the **defaults** portion of the statement.

The format for extended **community-ids** is the following:

```
type:administrator:assigned-number
```

**type** is the type of extended community and can be either a **bandwidth**, **target**, **origin**, **domain-id**, **src-as**, or **rt-import** community or a 16-bit number that identifies a specific BGP extended community. The **target** community identifies the destination to which the route is going. The **origin** community identifies where the route originated. The **domain-id** community identifies the OSPF domain from which the route originated. The **src-as** community identifies the autonomous system from which the route originated. The **rt-import** community identifies the route to install in the routing table.

**NOTE:** For **src-as**, you can specify only an AS number and not an IP address. For **rt-import**, you can specify only an IP address and not an AS number.

**administrator** is the administrator. It is either an AS number or an IPv4 address prefix, depending on the type of extended community.

**assigned-number** identifies the local provider.

The format for linking a bandwidth with an AS number is:

```
bandswidth:as-number:bandwidth
```

**as-number** specifies the AS number and **bandwidth** specifies the bandwidth in bytes per second.
NOTE: In Junos OS Release 9.1 and later, you can specify 4-byte AS numbers as defined in RFC 4893, BGP Support for Four-octet AS Number Space, as well as the 2-byte AS numbers that are supported in earlier releases of the Junos OS. In plain-number format, you can configure a value in the range from 1 through 4,294,967,295. To configure a target or origin extended community that includes a 4-byte AS number in the plain-number format, append the letter “L” to the end of number. For example, a target community with the 4-byte AS number 334,324 and an assigned number of 132 is represented as target:334324L:132.

In Junos OS Release 9.2 and later, you can also use AS-dot notation when defining a 4-byte AS number for the target and origin extended communities. Specify two integers joined by a period: **16-bit high-order value in decimal.16-bit low-order value in decimal**. For example, the 4-byte AS number represented in plain-number format as 65546 is represented in AS-dot notation as 1.10.

As defined in RFC 8092, BGP large community uses 12-byte encoding and the format for BGP large community-ids is:

```
large: global-administrator:assigned-number:assigned-number
```

- **large** indicates BGP large community.
- **global-administrator** is the administrator. It is a 4-byte AS number.
- **assigned-number** is a 4-byte value used to identify the local provider. BGP large community uses two 4-byte assigned number to identify the local provider.

**Required Privilege Level**

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

**Related Documentation**

- Understanding BGP Communities, Extended Communities, and Large Communities as Routing Policy Match Conditions
- Understanding How to Define BGP Communities and Extended Communities
- `dynamic-db`
**compatibility-mode**

**Syntax**

compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate value>;

**Hierarchy Level**

[edit interfaces interface-name e3-options], [edit interfaces interface-name t3-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure the E3 or T3 interface to be compatible with the channel service unit (CSU) at the remote end of the line.

---

**NOTE:** The compatibility-mode statement at the [edit interfaces interface-name e3-options] hierarchy level is not valid for IQE PICs.

---

**Default**

If you omit this option, the full E3 or T3 rate is used.

**Options**

- **adtran**—For T3 IQ interfaces only, configure compatibility with Adtran CSUs.
- **digital-link**—Configure compatibility with Digital Link CSUs. If you include this option on an E3 interface, you must also disable payload scrambling.
- **kentrox**—Configure compatibility with Kentrox CSUs. Kentrox subrate is valid for E3 IQ and T3 IQ interfaces only.
- **larscom**—For T3 and T3 IQ interfaces only, configure compatibility with Larscom CSUs.
- **verilink**—For T3 IQ and T3 IQE interfaces only, configure compatibility with Verilink CSUs.

---

**NOTE:** Verilink configuration is not functional if an IQ interface is paired with an IQE interface.

---

**subrate value**—Subrate of the E3 or T3 line.

**Range:** For Kentrox CSUs on E3 IQ interfaces and T3 IQ interfaces the subrate value must match the value configured on the CSU. Each increment of the subrate value corresponds to a rate increment of about 0.5 Mbps.

**Required Privilege Level**

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.
Related Documentation

- Configuring the E3 CSU Compatibility Mode
- Configuring the T3 CSU Compatibility Mode
- payload-scrambler on page 838

**compression (PPP Properties)**

Syntax

```plaintext
compression {
  acfc;
  pfc;
}
```

Hierarchy Level

- `[edit interfaces interface-name ppp-options]`
- `[edit interfaces interface-name unit logical-unit-number ppp-options]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]`

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For interfaces with PPP encapsulation, set Link Control Protocol (LCP) compression 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

- Configuring PPP Address and Control Field Compression on page 133
- Configuring the PPP Protocol Field Compression on page 135
compression (Voice Services)

Syntax

```
compression {
  rtp {
    f-max-period number;
    queues [ queue-numbers ];
    port {
      minimum port-number;
      maximum port-number;
    }
  }
}
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the compression properties for voice services traffic.

The remaining statements are described separately.

Required Privilege

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

Related Documentation

• Junos OS Services Interfaces Library for Routing Devices
**compression-device**

**Syntax**

```text
compression-device interface-name;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Specify the compression interface for voice services traffic.

**Options**

`interface-name`—Logical interface used for compression.

**Required Privilege Level**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

**Related Documentation**

- Junos OS Services Interfaces Library for Routing Devices
- Junos OS Interfaces and Routing Configuration Guide

**connections**

**Syntax**

```text
connections {
  interface-switch connection-name {
    interface interface-name.unit-number;
    interface interface-name.unit-number;
  }
}
```

**Hierarchy Level**

```
[edit protocols]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Define the connection between two circuits in a circuit cross-connect (CCC) connection. 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**

- Defining the Connection for Switching Cross-Connects on page 261
- MPLS Applications Feature Guide
connection-protection-tlv

Syntax
connection-protection-tlv;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name continuity-check]

Description
Includes connection protection OUI TLV in continuity check messages (CCM). The TLV
is responsible for carrying the flag information within CCM PDUs. Though this OUI TLV
will be included in the CCM frames by provider edge devices, the value is updated by the
provider routers in case the traffic to the other end of the network is forwarded by the
facility protection tunnel.

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

Related Documentation
• connectivity-fault-management on page 482
• Configuring MAC Flush Message Processing in CET Mode
• Example: Configuring an Action Profile Based on Connection Protection TLVs
connectivity-fault-management

Syntax

```
connectivity-fault-management {
  action-profile profile-name {
    action {
      interface-down;
      log-and-generate-ais {
        interval(1m | 1s);
        level value;
        priority value;
      }
    }
    default-actions {
      interface-down;
    }
    event {
      ais-trigger-condition {
        adjacency-loss;
        all-defects;
        cross-connect-ccm;
        erroneous-ccm;
        receive-ais;
      }
      adjacency-loss;
      interface-status-tlv (down | lower-layer-down);
      port-status-tlv blocked;
      rdi;
    }
  }
  linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
  }
  expected-defect {
    rx-enable;
    rx-max-duration seconds;
    tx-enable;
    tx-duration seconds;
  }
  maintenance-domain domain-name {
    bridge-domain <vlan-id [ vlan-ids ]>;
    instance routing-instance-name;
    interface interface-name;
    level number;
    name-format (character-string | none | dns | mac+2oct);
    maintenance-association ma-name {
      protect-maintenance-association protect-ma-name;
      remote-maintenance-association remote-ma-name;
      short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
      continuity-check {
        convey-loss-threshold;
        hold-interval minutes;
        interface-status-tlv;
      }
    }
  }
}
```
interval (10m | 10s | 1m | 1s | 100ms);
loss-threshold number;
port-status-tlv;
}
mep mep-id {
  auto-discovery;
direction (up | down);
interface interface-name (protect | working);
lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
  rem-err-xcon | xcon);
priority number;
remote-mep mep-id {
  action-profile profile-name;
  sla-iterator-profile profile-name {
    data-tlv-size size;
    iteration-count count value;
    priority priority-value;
detect-loc;
  }
}
}
}
virtual-switch routing-instance-name {
  bridge-domain name <vlan-ids [ vlan-ids ]>;
}
}
no-aggregate-delegate-processing;
performance-monitoring {
  delegate-server-processing;
hardware-assisted-timestamping;
hardware-assisted-keepalives;
sla-iterator-profiles {
  profile-name {
    avg-fd-twoway-threshold;
    avg-ifdv-twoway-threshold;
    avg-flr-forward-threshold;
    avg-flr-backward-threshold;
disable;
calculation-weight {
  delay delay-weight;
delay-variation delay-variation-weight;
}
cycle-time milliseconds;
iteration-period connections;
measurement-type (loss | statistical-frame-loss | two-way-delay);
}
}
}
}

Hierarchy Level   [edit protocols oam ethernet]

Release Information Statement introduced in Junos OS Release 8.4.
Description  For Ethernet interfaces on M7i and M10i routers with Enhanced CFEB (CFEB-E), and on M120, M320, MX Series, and T Series routers, specify connectivity fault management for IEEE 802.1ag Operation, Administration, and Management (OAM) support. In Junos OS Release 9.3 and later, this statement is also supported on aggregated Ethernet interfaces.

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  • IEEE 802.1ag OAM Connectivity Fault Management Overview

container-devices

Syntax  container-devices {
  device-count number;
}

Hierarchy Level  [edit chassis]


Description  Specify the container devices configuration. The number option specifies the number of sequentially numbered container interfaces, from ci0 to ci127 maximum.

Options  number—Number of container devices.
  Range: 1 through 128

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

Related Documentation  • Displaying APS Using a Container Interface with ATM Encapsulation
  • Configuring Container Interfaces for APS on SONET Links
**container-list**

**Syntax**  
container-list [ container-interface-names ];

**Hierarchy Level**  
[edit interfaces container-options]

**Release Information**  
Statement introduced in Junos OS Release 9.2.

**Description**  
Specify a list of container interfaces; for example: ci0, ci1, and up to ci127.

**Options**  
container-interface-names—Name of each container interface.

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

**Related Documentation**  
- Displaying APS Using a Container Interface with ATM Encapsulation  
- Configuring Container Interfaces for APS on SONET Links  
- container-options on page 486
container-options

Syntax  
container-options  
   container-list  
   container-interface-names  
   container-type  
   container-interface-names  
   member-interface-type  
   member-interface-names  
   member-interface-speed  
   member-interface-names  

Hierarchy Level  [edit interfaces]


Description  Specify the container interface options.

Options  
   interface-name—Name of the SONET or the container interface.
   aps—Specify the member link interface type of the container as APS.
   sonet—Protocol type of the container interface.
   speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation  
   • Displaying APS Using a Container Interface with ATM Encapsulation
   • Configuring Container Interfaces for APS on SONET Links
## container-type

**Syntax**

container-type *aps*;

**Hierarchy Level**

[edit interfaces container-options]

**Release Information**

Statement introduced in Junos OS Release 9.2.

**Description**

Specify the container-options interface type.

**Options**

*aps*—Configure the interface type to be Automatic Protection Switching (APS).

**Required Privilege**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Displaying APS Using a Container Interface with ATM Encapsulation
- Configuring Container Interfaces for APS on SONET Links
**continuity-check**

**Syntax**

```
continuity-check {
    convey-loss-threshold;
    hold-interval minutes;
    interface-status-tlv;
    interval (10m | 10s | 1m | 1s | 100ms | 10ms);
    loss-threshold number;
    port-status-tlv;
}
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.4.

**Description**

Specify continuity check protocol options.

**Options**

- `hold-interval minutes`—Specify the continuity check hold-interval, in minutes.
- `interface-status-tlv`—Enable interface-status-tlv transmission.
- `interval (10m | 10s | 1m | 1s | 100ms | 10ms)`—Specify the continuity check interval.
- `loss-threshold minutes`—Specify the loss-threshold, in minutes.
- `port-status-tlv`—Enable port-status-tlv transmission.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Continuity Check Protocol Parameters for Fault Detection
control-channel

Syntax
control-channel channel-name {
  vlan vlan-id;
  interface name interface-name
}

Hierarchy Level
[edit protocols protection-group ethernet-ring name (east-interface | west-interface)]

Release Information
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure the Ethernet RPS control channel logical interface to carry the RAPS PDU. The related physical interface is the physical ring port.

Options
vlan vlan-id—If the control channel logical interface is a trunk port, then a dedicated vlan vlan-id defines the dedicated VLAN channel to carry the RAPS traffic. Only configure the vlan-id when the control channel logical interface is the trunk port.

interface name interface-name—Interface name of the control channel.

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

Related Documentation
• Ethernet Ring Protection Switching Overview
• Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
• Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
• Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
**control-polarity**

**Syntax**

```
control-polarity (negative | positive);
```

**Hierarchy Level**

```
[edit interfaces interface-name serial-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For X.21 interfaces only, configure the control signal polarity.

**Options**

- `positive`—Positive signal polarity.
- `negative`—Negative signal polarity.

**Default**

`positive`

**Required Privilege Level**

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

**Related Documentation**

- Configuring Serial Signal Polarities on page 327
**control-signal**

**Syntax**

control-signal (assert | de-assert | normal);

**Hierarchy Level**

[edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For X.21 interfaces only, configure the to-DCE signal.

**Options**

*assert*—The to-DCE signal must be asserted.

*de-assert*—The to-DCE signal must be deasserted.

*normal*—Normal request-to-send (RTS) signal handling, as defined by ITU-T Recommendation X.21.

**Default:** normal

**Required Privilege**

**Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Configuring the Serial Signal Handling on page 324
copy-tos-to-outer-ip-header

**Syntax**

```
copy-tos-to-outer-ip-header;
```

**Hierarchy Level**

```
[edit interfaces at fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces at fpc/pic/port unit logical-unit-number]
```

**Release Information**

Statement introduced in Junos OS Release 8.2.

**Description**

For GRE tunnel interfaces only, enable the inner IP header's TOS bits to be copied to the outer IP packet header.

**Default**

If you omit this statement, the TOS bits in the outer IP header are set to 0.

**Required Privilege**

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

**Related Documentation**

- *Class of Service Feature Guide (Routers and EX9200 Switches)*

---

core-dump

**Syntax**

```
(core-dump | no-core-dump);
```

**Hierarchy Level**

```
[edit interfaces mo-fpc/pic/port multiservice-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For monitoring services interfaces only, a useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory `/var/tmp` contains core files. The Junos OS saves the current core file (0) and the four previous core files, which are numbered 1 through 4 (from newest to oldest):

- `core-dump`—Enable the core dumping operation.
- `no-core-dump`—Disable the core dumping operation.

**Required Privilege**

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

**Related Documentation**

- Configuring Multiservice Physical Interface Properties on page 154
- *Junos OS Services Interfaces Library for Routing Devices*
**crc-major-alarm-threshold**

**Syntax**

crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);

**Hierarchy Level**

[edit interfaces interface-name t1-options]

**Release Information**

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**

Major alarm error thresholds for T1 CRC errors. When the threshold is exceeded for one second, a defect condition is declared. If the defect condition continues for the monitoring period, an alarm condition is declared.

**Default**

10-second monitoring period for all settings except 1e-5. The 1e-5 value uses a 50-second monitoring period.

**Options**

1e-3—Error rate expressed as the number of errors per number of bits. The value 1e-3 is one crc error in 10^3 bits.

1e-4—Error rate expressed as the number of errors per number of bits. The value 1e-4 is one crc error in 10^4 bits.

1e-5—Error rate expressed as the number of errors per number of bits. The value 1e-5 is one crc error in 10^5 bits.

5e-4—Error rate expressed as the number of errors per number of bits. The value 5e-4 is five crc errors in 10^4 bits.

5e-5—Error rate expressed as the number of errors per number of bits. The value 5e-5 is five crc errors in 10^5 bits.

**Required Privilege Level**

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

**Related Documentation**

- Configuring T1 CRC Error Major Alarm Thresholds
crc-minor-alarm-threshold

Syntax:  
crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);

Hierarchy Level:  
[edit interfaces interface-name t1-options]

Release Information:  
Statement introduced in Junos OS Release 8.5.  
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description:  
Minor alarm error thresholds for T1 CRC errors. When the threshold is exceeded for one second, a defect condition is declared. If the defect condition continues for the monitoring period, an alarm condition is declared.

Default:  
10-second monitoring period for values 1e-3, 5e-4, 1e-4, and 5e-5. The 1e-5 value uses a 50-second monitoring period. The 5e-6 value uses a 100-second monitoring period. The 1e-6 value uses a 500-second monitoring period.

Options:  
1e-3—Error rate expressed as the number of errors per number of bits. The value 1e-3 is one crc error in 10^3 bits.

1e-4—Error rate expressed as the number of errors per number of bits. The value 1e-4 is one crc error in 10^4 bits.

1e-5—Error rate expressed as the number of errors per number of bits. The value 1e-5 is one crc error in 10^5 bits.

1e-6—Error rate expressed as the number of errors per number of bits. The value 1e-6 is one crc error in 10^6 bits.

5e-4—Error rate expressed as the number of errors per number of bits. The value 5e-4 is five crc errors in 10^4 bits.

5e-5—Error rate expressed as the number of errors per number of bits. The value 5e-5 is five crc errors in 10^5 bits.

5e-6—Error rate expressed as the number of errors per number of bits. The value 5e-6 is five crc errors in 10^6 bits.

Default: 5e-6

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

Related Documentation:  
• Configuring T1 CRC Error Minor Alarm Thresholds
**cts**

**Syntax**

```plaintext
ccts (ignore | normal | require);
```

**Hierarchy Level**

```plaintext
[edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For EIA-530 and V.35 interfaces only, configure the from-DCE signal, clear-to-send (CTS).

**Options**

- **ignore**—The from-DCE signal is ignored.
- **normal**—Normal CTS signal handling as defined by the TIA/EIA Standard 530.
- **require**—The from-DCE signal must be asserted.

**Default:** normal

**Required Privilege**

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

**Related Documentation**

- Configuring the Serial Signal Handling on page 324
**cts-polarity**

**Syntax**  
cts-polarity (negative | positive);

**Hierarchy Level**  
[edit interfaces interface-name serial-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
Configure CTS signal polarity.

**Options**  
positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

**Required Privilege Level**  
interface—To view this statement in the configuration.

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

**Related Documentation**  
• Configuring Serial Signal Polarities on page 327
cycle-time

Syntax:  
```
cycle-time cycle-time-value;
```

Hierarchy Level:  
```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]
```

Release Information:  
Statement introduced in Junos OS Release 11.1.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description:  
Configure the time (in milliseconds) taken between back-to-back transmissions of SLA frames for a single connection.

Options:  
cycle-time-value—Cycle time value in milliseconds.  
Range:  10 through 3,600,000  
Default:  1000

Required Privilege:  
Configure—To enter configuration mode.  
Control—To modify any configuration.

Related Documentation:  
- Configuring an Iterator Profile  
- Configuring an Iterator Profile on a Switch (CLI Procedure)
damping (Interfaces)

Syntax
damping {
    enable;
    half-life seconds;
    max-suppress seconds;
    reuse number;
    suppress number;
}

Hierarchy Level
[edit interfaces interface--name],
[edit interfaces interface--range]

Release Information
Statement introduced in Junos OS Release 14.1 for PTX Series Packet Transport Routers and T Series Core Routers.

Description
Limit the number of advertisements of the up and down transitions (flapping) on an interface. Each time a transition occurs, the interface state is changed, which generates an advertisement to the upper-level routing protocols. Damping helps reduce the number of these advertisements. Every time an interface goes down, a penalty is added to the interface penalty counter. Penalty added on every interface flap is 1000.

If at some point the accumulated penalty exceeds the suppress level max-suppress, the interface is placed in the suppress state, and further interface state up and down transitions are not reported to the upper-level protocols.

Options
enable—Enable damping on a per-interface basis. If damping is enabled on an interface, it is suppressed during interface flaps that match the configuration settings.

Default: Disabled

half-life seconds—Decay half-life. seconds is the interval after which the accumulated interface penalty counter is reduced by half if the interface remains stable.

Range: 1 through 30
Default: 5

max-suppress seconds—Maximum hold-down time. seconds is the maximum time that an interface can be suppressed no matter how unstable the interface has been.

NOTE: For the half-life, configure a value that is less than the max-suppress value. If you do not, the configuration is rejected.
NOTE: For max-suppress, configure a value that is greater than the half-life. If you do not, the configuration is rejected.

Range: 1 through 20,000
Default: 20

**reuse number**—Reuse threshold. When the accumulated interface penalty counter falls below *number*, the interface is no longer suppressed.

Range: 1 through 20,000
Default: 1000

**suppress number**—Cutoff (suppression) threshold. When the accumulated interface penalty counter exceeds *number*, the interface is suppressed.

Range: 1 through 20,000
Default: 2000

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

**Related Documentation**
- Physical Interface Damping Overview on page 143
- Damping Shorter Physical Interface Transitions on page 149
- Damping Longer Physical Interface Transitions on page 150
- show interfaces extensive on page 1613
- hold-time on page 646
**data-channel**

**Syntax**
```
data-channel {
  vlan number;
}
```

**Hierarchy Level**
```
[edit protocols protection-group ethernet-ring ring-name]
```

**Release Information**
Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**
For Ethernet ring protection, configure a data channel to define a set of VLAN IDs that belong to a ring instance.

VLANs specified in the data channel use the same topology used by the ERPS PDU in the control channel. Therefore, if a ring interface is blocked in the control channel, all traffic in the data channel is also blocked on that interface.

**Options**
- **vlan number**—Specify (by VLAN ID) one or more VLANs that belong to a ring instance.

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

**Related Documentation**
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers
- Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
- Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
# data-tlv-size

## Syntax

data-tlv-size size;

## Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile profile-name]
```

## Release Information

Statement introduced in Junos OS Release 11.1.

## Description

Configure the size of the data TLV portion of the Y.1731 data frame.

## Options

- **size**—Size of the data TLV portion of the Y.1731 data frame.

**NOTE:** This option is applicable only for two-way delay measurement.

- **Range:** 1 through 1400 bytes
- **Default:** 1

## Required Privilege Level

- **Configure**—To enter configuration mode.
- **Control**—To modify any configuration.

## Related Documentation

- sla-iterator-profile on page 998
- Configuring a Remote MEP with an Iterator Profile
dcd

Syntax  dcd (ignore | normal | require);

Hierarchy Level  [edit interfaces interface-name serial-options dce-options],
                 [edit interfaces interface-name serial-options dte-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For EIA-530 and V.35 interfaces only, configure the from-DCE signal, data-carrier-detect (DCD).

Options  ignore—The from-DCE signal is ignored.
         normal—Normal DCD signal handling as defined by the TIA/EIA Standard 530.
         require—The from-DCE signal must be asserted.
         Default: normal

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

Related Documentation  • Configuring the Serial Signal Handling on page 324
dc-d polarity

Syntax  dc-d polarity (negative | positive);

Hierarchy Level  [edit interfaces interface-name serial-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure DCD signal polarity.

Options  positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

Required Privilege  Level

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring Serial Signal Polarities on page 327

dce

Syntax  dce;

Hierarchy Level  [edit interfaces interface-name],

[edit interfaces interface-name serial-options clocking-mode]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For Frame Relay only, respond to status enquiry message keepalives.

When you configure the router to be a DCE, keepalives are disabled by default.

Default  The router operates in DTE mode.

Required Privilege  Level

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring the Router as a DCE with Frame Relay Encapsulation on page 138
**deactivation-delay**

**Syntax**

deeacti\ion-delay seconds;

**Hierarchy Level**

[edit interfaces dl\n unit logical-unit-number dialer-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

On J Series Services Routers with ISDN interfaces, configure the ISDN deactivation delay. Used only for dialer backup and dialer watch cases.

**Options**

seconds—Interval before the backup interface is deactivated after the primary interface has comes up.

Range: 1 through 4,294,967,295 seconds

Default: 0 (zero)

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide
dce-options

Syntax

dce-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}

Hierarchy Level

[edit interfaces interface-name serial-options]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement previously known as control-leads.

Description
For J Series Services Routers, configure the serial interface signal characteristics.
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 Serial Signal Handling on page 324
default-actions

**Syntax**

```
default-actions [interface-down;]
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.4.

**Description**

Define the action to be taken when connectivity to the remote MEP is lost.

**Default**

If no action is configured, no action is taken.

**Options**

**interface-down**—When a remote MEP connectivity failure is detected, bring the interface down.

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- *Configuring a CFM Action Profile to Specify CFM Actions for CFM Events*
default-chap-secret

Syntax  
default-chap-secret name;

Hierarchy Level  
[edit interfaces interface-name ppp-options chap],
[edit interfaces interface-name unit logical-unit-number ppp-options chap],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options chap]

Release Information  
Statement introduced in Junos OS Release 8.0.

Description  
Define the default CHAP secret to be used when no matching CHAP access profile exists.

For ATM2 IQ interfaces only, you can configure a default CHAP secret on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

• atm-ppp-llc—PPP over AAL5 LLC encapsulation.
• atm-ppp-vc-mux—PPP over AAL5 multiplex encapsulation.

Default  
If you do not include the default-chap-secret statement in the configuration, and an interface receives a CHAP challenge or response from a peer that is not in the applied access profile, the link is immediately dropped.

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

Related Documentation  
• Configuring a Default CHAP Secret
• access-profile on page 394
**default-pap-password**

**Syntax**
```
default-pap-password password;
```

**Hierarchy Level**
- [edit interfaces interface-name unit logical-unit-number ppp-options pap],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options pap]

**Release Information**
Statement introduced in Junos OS Release 8.3.

**Description**
For PAP authentication, the default PAP password.

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

**Related Documentation**
- Configuring a Default PAP Password
- access-profile on page 394

**delimiter**

**Syntax**
```
delimiter delimiter-character;
```

**Hierarchy Level**
- [edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
- [edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include]

**Release Information**
Statement introduced in Junos OS Release 10.0.

**Description**
Specify the character used as the delimiter between the concatenated components of the username. You cannot use the semicolon (;) as a delimiter.

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

**Related Documentation**
- Configuring VLAN Interface Username Information for AAA Authentication
demux-destination (Underlying Interface)

Syntax  
demux-destination family;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name interfaces interface-name unit logical-unit-number]

Release Information  
Statement introduced in Junos OS Release 9.0.
Support for aggregated Ethernet added in Junos OS Release 9.4.

Description  
Configure the logical demultiplexing (demux) destination family type on the IP demux underlying interface.

NOTE: The IP demux interface feature currently supports only Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.

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

Related Documentation
• Configuring an IP Demultiplexing Interface on page 296
• Configuring a VLAN Demultiplexing Interface on page 301
# demux-destination (Demux Interface)

**Syntax**
```
demux-destination {
  destination-prefix;
}
```

**Hierarchy Level**
- [edit interfaces interface-name unit logical-unit-number family family],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family],
- [edit logical-systems logical-system-name routing-instances routing-instance-name interfaces interface-name unit logical-unit-number family family]

**Release Information**
Statement introduced in Junos OS Release 9.0.
Support for aggregated Ethernet added in Junos OS Release 9.4.

**Description**
Configure one or more logical demultiplexing (demux) destination prefixes. The prefixes are matched against the destination address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

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

**Related Documentation**
- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
**demux-options (Static Interface)**

**Syntax**

```
demux-options {
  underlying-interface interface-name
}
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced in Junos OS Release 9.0.

**Description**

Configure logical demultiplexing (demux) interface options.

The remaining statement is explained separately. See CLI Explorer.

**Required Privilege**

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

**Related Documentation**

- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
demux-source (Demux Interface)

Syntax

```
demux-source {
    source-prefix;
}
```

Hierarchy Level

- [edit interfaces interface-name unit logical-unit-number family family],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family],
- [edit logical-systems logical-system-name routing-instances routing-instance-name interfaces interface-name unit logical-unit-number family family]

Release Information

Statement introduced in Junos OS Release 9.0.
Support for aggregated Ethernet added in Junos OS Release 9.4.

Description

Configure one or more logical demultiplexing (demux) source prefixes. The prefixes are matched against the source address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the demux interface.

Required Privilege Level

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

Related Documentation

- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
demux-source (Underlying Interface)

Syntax  
```
demux-source family;
```

Hierarchy Level  
```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name interfaces interface-name unit logical-unit-number]
```

Release Information  
Statement introduced in Junos OS Release 9.0.  
Support for aggregated Ethernet added in Junos OS Release 9.4.

Description  
Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface.

NOTE: The IP demux interface feature currently supports only Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.

Options  
```
family—Protocol family:
  • inet—Internet Protocol version 4 suite
  • inet6—Internet Protocol version 6 suite
```

Required Privilege  
```
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
```

Related Documentation  
```
  • Configuring an IP Demultiplexing Interface on page 296
  • Configuring a VLAN Demultiplexing Interface on page 301
```
demux0 (Static Interface)

Syntax

```plaintext
demux0 { 
    unit logical-unit-number { 
        demux-options { 
            underlying-interface interface-name 
        }
        family family { 
            access-concentrator name; 
            { 
                destination-prefix; 
            }
            direct-connect; 
            duplicate-protection; 
            dynamic-profile profile-name; 
            { 
                source-prefix; 
            }
            max-sessions number; 
            service-name-table table-name 
            targeted-distribution; 
            unnumbered-address interface-name <preferred-source-address address>; 
        }
        vlan-id number; 
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id]; 
    }
}
```

Hierarchy Level

- [edit interfaces].
- [edit logical-systems logical-system-name interfaces]

Release Information

Statement introduced in Junos OS Release 9.0.

Description

Configure the logical demultiplexing (demux) interface.

Logical IP demux interfaces do not support IPv4 and IPv6 dual stack.

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 an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
demux0 (Dynamic Interface)

Syntax

demux0
    unit logical-unit-number
        demux-options
            underlying-interface interface-name
    family family
        access-concentrator name;
        address address;
        demux-source
            source-prefix;
        direct-connect;
        duplicate-protection;
        dynamic-profile profile-name;
        filter
            input filter-name;
            output filter-name;
        mac-validate (loose | strict):
            max-sessions number;
            max-sessions-vsa-ignore;
        rpf-check
            fail-filter filter-name;
            mode loose;
        service-name-table table-name
            short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max maximum-seconds>
            unnumbered-address interface-name <preferred-source-address address>;
    filter
        input filter-name;
        output filter-name;
    vlan-id number;
}

Hierarchy Level
[edit dynamic-profiles profile-name interfaces]

Release Information
Statement introduced in Junos OS Release 9.3.

Description
Configure the logical demultiplexing (demux) interface in a dynamic profile.

Logical IP demux interfaces do not support IPv4 and IPv6 dual stack.

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**
- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles
- Demultiplexing Interface Overview on page 293
description (Interfaces)

Syntax

```
description text;
```

Hierarchy Level

```
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

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 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Provide a textual description of the interface or the logical unit. Any descriptive text you include is displayed in the output of the `show interfaces` commands, and is also exposed in the `ifAlias` Management Information Base (MIB) object. It has no effect on the operation of the interface on the router or switch.

The textual description can also be included in the extended DHCP relay option 82 Agent Circuit ID suboption.

Options

```
text—Text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks.
```

Required Privilege

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

Related Documentation

- Configuring Interface Description on page 98
- Adding a Logical Unit Description to the Configuration on page 172
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit and 10-Gigabit Ethernet Interfaces for OCX Series Switches
- Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support
- Configuring Gigabit and 10-Gigabit Ethernet Interfaces for EX4600 and QFX Series Switches
- Using DHCP Relay Agent Option 82 Information
- Junos OS Network Interfaces Library for Routing Devices
- Example: Connecting Access Switches with ELS Support to a Distribution Switch with ELS Support
destination (IPCP)

Syntax

```
destination address destination-profile profile-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For unnumbered interfaces with PPP encapsulation, specify the IP address of the remote interface.

Options

`address`—IP address of the remote interface.

The remaining statement is 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 IPCP Options for Interfaces with PPP Encapsulation on page 200
- address on page 407
- negotiate-address on page 818
- Junos OS Administration Library
**destination (Routing Instance)**

**Syntax**

destination routing-instance-name;

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number tunnel routing-instance],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel routing-instance]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Specify the destination routing instance that points to the routing table containing the tunnel destination address.

**Default**

The default Internet routing table inet.0.

**Required Privilege Level**

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

**Related Documentation**

• Junos OS Services Interfaces Library for Routing Devices
destination (Tunnels)

Syntax

```
destination address;
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet address address],
[edit interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name],
[edit interfaces interface-name unit logical-unit-number tunnel],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

For encrypted, PPP-encapsulated, and tunnel interfaces, specify the remote address of the connection.

Options

```
address—Address of the remote side of the connection.
```

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 Address on page 191
- Configuring Generic Routing Encapsulation Tunneling
- Junos OS Services Interfaces Library for Routing Devices
destination-class-usage

Syntax  destination-class-usage;

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

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Enable packet counters on an interface that count packets that arrive from specific customers and are destined for specific prefixes on the provider core router.

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

Related Documentation  •  Enabling Source Class and Destination Class Usage on page 241
  •  accounting on page 395
  •  source-class-usage on page 1006
destination-profile

Syntax  
destination-profile name;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number family inet address address],
[edit interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name destination address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet unnumbered-address interface-name destination address]

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

Description  
For interfaces with PPP encapsulation, assign PPP properties to the remote destination end. You define the profile at the [edit access group-profile name ppp] hierarchy level.

Options  
name—Profile name defined at the [edit access group-profile name ppp] 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 IPCP Options for Interfaces with PPP Encapsulation on page 200
- destination (IPCP) on page 518
- Junos OS Administration Library
dial-options

Syntax
dial-options {
  ipsec-interface-id name;
  l2tp-interface-id name;
  (shared | dedicated);
}

Hierarchy Level
[edit interfaces sp-fpc/pic/port unit logical-unit-number],
[edit interfaces si-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces sp-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces si-fpc/pic/port unit logical-unit-number]

Release Information
Statement introduced before Junos OS Release 7.4.
The [edit ...si-...] hierarchy levels introduced in Junos OS Release 11.4.

Description
Specify the options for configuring logical interfaces for group and user sessions in L2TP or IPsec dynamic endpoint tunneling.

Options
dedicated—(LNS on M Series routers and MX Series routers only) Specify that a logical interface can host only one session at a time.

ipsec-interface-id name—(M Series routers only) Interface identifier for group of dynamic peers. This identifier must be replicated at the [edit access profile name client * ike] hierarchy level.

l2tp-interface-id name—Interface identifier that must be replicated at the [edit access profile name] hierarchy level.

shared—(LNS on M Series routers only) Specify that a logical interface can host multiple (shared) sessions at a time.

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

Related Documentation
• Configuring the Identifier for Logical Interfaces that Provide L2TP Services
• Configuring Dynamic Endpoints for IPsec Tunnels
• Configuring Options for the LNS Inline Services Logical Interface
**dial-string**

**Syntax**

dial-string [ dial-string-numbers ];

**Hierarchy Level**

[edit interfaces br-pim/0/port unit logical-unit-number dialer-options],
[edit logical-systems logical-system-name interfaces br-pim/0/port unit logical-unit-number dialer-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

On J Series Services Routers with ISDN interfaces, specify one or more ISDN dial strings used to reach a destination subnetwork.

**Options**

*dial-string-numbers*—One or more strings of numbers to call.

**Required Privilege**

interface—To view this statement in the configuration.

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

**Related Documentation**

None

---

**dialer**

**Syntax**

dialer filter-name;

**Hierarchy Level**

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

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Apply a dialer filter to an interface. To create the dialer filter, include the *dialer-filter* statement at the [edit firewall filter family family] hierarchy level.

**Options**

*filter-name*—Dialer filter name.

**Required Privilege**

interface—To view this statement in the configuration.

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

**Related Documentation**

- *Junos OS Interfaces and Routing Configuration Guide*
dialer-options

Syntax
dialer-options {
activation-delay seconds;
callback;
callback-wait-period time;
deactivation-delay seconds;
dial-string [ dial-string-numbers ];
idle-timeout seconds;
ingoing-map {
caller caller-number | accept-all;
initial-route-check seconds;
load-interval seconds;
load-threshold percent;
pool pool-name;
redial-delay time;
watch-list {
[ routes ];
}
}
}

Hierarchy Level
[edit interfaces umd0],
[edit interfaces dl unit logical-unit-number],
[edit logical-systems logical-system-name interfaces dl unit logical-unit-number]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the dialer options for configuring logical interfaces for group and user sessions.
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
• Junos OS Services Interfaces Library for Routing Devices
dialin

Syntax    dialin (console | routable);

Hierarchy Level    [edit interfaces umd0 modem-options]

Release Information    Statement introduced in Junos OS Release 8.5.

Description    For J Series Services Routers, configure a USB modem port to act as a dial-in console or WAN backup port.

Options    

    console—Configure the USB modem port to operate as a dial-in console for management.

    routable—Configure the USB modem port to operate as a dial-in WAN backup interface.

    Default: console

Required Privilege Level    interface—To view this statement in the configuration.

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

Related Documentation    • Specifying a USB Modem Interface on J Series Routers on page 331
direction

Syntax  
direction (up | down);

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management maintenance-domain  
domain-name maintenance-association ma-name mep mep-id]

Release Information  
Statement introduced in Junos OS Release 8.4.

Description  
Configure the direction of the MEP.

Options  
up—An UP MEP CCM is transmitted out of every logical interface which is part of the  
same bridging or vpls instance except for the interface configured on this MEP.

NOTE:  The up direction for MEP is not supported on T Series routers.

down—Down MEP CCMs are transmitted only out the interface configured on this MEP.

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

Related Documentation  
• Configuring a MEP to Generate and Respond to CFM Protocol Messages  
• IEEE 802.1ag OAM Connectivity Fault Management Overview
disable (Interface)

Syntax

disable;

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

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 12.2 for ACX Series Universal Metro Routers.

Description

Disable a physical or a logical interface, effectively unconfiguring it.

CAUTION:

- Dynamic subscribers and logical interfaces use physical interfaces for connection to the network. The Junos OS allows you to set the interface to disable and commit the change while dynamic subscribers and logical interfaces are still active. This action results in the loss of all subscriber connections on the interface. Use care when disabling interfaces.

- If aggregated SONET links are configured between a T1600 router and a T4000 router, interface traffic is disrupted when you disable the physical interface configured on the T1600 router. If you want to remove the interface, we recommend that you deactivate the interface instead of disabling it.

NOTE:

- When you use the disable statement at the [edit interfaces] hierarchy level, depending on the PIC type, the interface might or might not turn off the laser. Older PIC transceivers do not support turning off the laser, but newer Gigabit Ethernet (GE) PICs with SFP and XFP transceivers and ATM MIC with SFP do support it and the laser will be turned off when the interface is disabled. If the ATM MIC with SFP is part of an APS group, then the laser will not be turned off when you use the disable statement at the [edit interfaces] hierarchy level.

- When you disable or deactivate an interface, then all the references made to the deactivated interface must be removed from the routing instance.

- For abstracted fabric interfaces, the disable command disables AF interface on the local GNF only.
**WARNING:** Do not stare into the laser beam or view it directly with optical instruments even if the interface has been disabled.

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

**Related Documentation**
- Disabling a Physical Interface on page 158
- Disabling a Logical Interface on page 185

### disable (Link Protection)

**Syntax**
disable;

**Hierarchy Level**
[edit interfaces aeX aggregated-ether-options lACP link-protection]

**Release Information**
Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.4 for EX Series switches.
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

**Description**
Disable LACP link protection on the interface.

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

**Related Documentation**
- Configuring LACP for Aggregated Ethernet Interfaces
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces for Switches
### disable-mlppp-inner-ppp-pfc

**Syntax**
```
disable-mlppp-inner-ppp-pfc;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**
Statement introduced in Junos OS Release 8.2.

**Description**
For MLPPP interfaces only, disable compression of the inner PPP header in the MLPPP payload. By default, compression is enabled.

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

**Related Documentation**
- *Junos OS Services Interfaces Library for Routing Devices*
dlci

Syntax  
\`dlci dlci-identifier;\`

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

Release Information  
Statement introduced before Junos OS Release 7.4.
Starting with Junos OS Release 18.2R1, the SRX Series devices support frame-relay encapsulation and adds DLCI information to the given frame.

Description  
For Frame Relay and Multilink Frame Relay (MLFR) user-to-network interface (UNI) network-to-network interface (NNI) encapsulation only, and for link services, voice services and point-to-point interfaces only, configure the data-link connection identifier (DLCI) for a permanent virtual circuit (PVC) or an switched virtual circuit (SVC). The DLCI setups a frame-relay PVC to form a L2 point-to-point connection. This is used for peering different LT IFL pairs.

To configure a DLCI for a point-to-multipoint interface, use the `multipoint-destination` statement to specify the DLCI.

Options  
`dlci-identifier`—Data-link connection identifier.
  
Range: 16 through 1022.

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

Related Documentation  
  
- Data-Link Connection Identifiers on Channelized Interfaces
- Configuring Frame Relay DLCIs
- Junos OS Services Interfaces Library for Routing Devices
- encapsulation (Logical Interface) on page 567
- multicast-dlcion page 802
- multipoint-destination on page 807
do-not-fragment

Syntax  do-not-fragment;

Hierarchy Level  [edit interfaces gr-fpc/pic/port unit logical-unit-number tunnel],
                 [edit logical-systems logical-system-name interfaces gr-fpc/pic/port unit logical-unit-number tunnel]

                      Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches.
                      Statement introduced in Junos OS Release 19.3 for MPC10E line card.

Description  For a generic routing encapsulation (GRE) tunnel, disable fragmentation of GRE-encapsulated packets. This sets the do-not-fragment (DF) bit in the outer IP header of the GRE-encapsulated packets so that they do not get fragmented anywhere in the path. When the size of a GRE-encapsulated packet is greater than the MTU of a link that the packet passes through, the GRE-encapsulated packet is dropped.

Default  By default, fragmentation of GRE-encapsulated packets is disabled.

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

Related Documentation  • allow-fragmentation on page 420
                       • reassemble-packets
                       • Enabling Fragmentation and Reassembly on Packets After GRE-Encapsulation
                       • Junos OS Services Interfaces Library for Routing Devices
**domain-name**

**Syntax**

```
domain-name domain-name-string;
```

**Hierarchy Level**

```
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.

**Description**

Specify the domain name that is concatenated with the username during the subscriber authentication process.

**Options**

`domain-name-string`—The 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**

- `Configuring VLAN Interface Username Information for AAA Authentication`
dot1x

Syntax  dot1x {
  authenticator {
    authentication-profile-name access-profile-name;
    interface interface-id {
      maximum-requests integer;
      quiet-period seconds;
      reauthentication (disable | interval seconds);
      retries integer;
      server-timeout seconds;
      supplicant (single);
      supplicant-timeout seconds;
      transmit-period seconds;
    }
  }
}

Hierarchy Level  [edit protocols]

Release Information  Statement introduced in Junos OS Release 9.3.

Description  For the MX Series only, specifies settings for using 802.1x Port-Based Network Access Control.

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

• IEEE 802.1x Port-Based Network Access Control Overview
• authenticator on page 434
• authentication-profile-name on page 433
• interface (IEEE 802.1x) on page 687
down-count

**Syntax**
```
down-count cells;
```

**Hierarchy Level**
- `[edit interfaces interface-name atm-options vpi vpi-identifier oam-liveness]`
- `[edit interfaces interface-name unit logical-unit-number oam-liveness]`
- `[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address oam-liveness]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number oam-liveness]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address multipoint-destination address oam-liveness]`

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For ATM encapsulation only, configure Operation, Administration, and Maintenance (OAM) F5 loopback cell count thresholds. This feature is not supported on ATM-over-SHDSL interfaces.

For ATM2 IQ PICs only, configure OAM F4 loopback cell count thresholds at the `[edit interfaces interface-name atm-options vpi vpi-identifier]` hierarchy level.

**Options**
- `cells`—Minimum number of consecutive OAM F4 or F5 loopback cells lost before a VC is declared down.
  - **Range:** 1 through 255
  - **Default:** 5 cells

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

**Related Documentation**
- *Configuring the ATM OAM F5 Loopback Cell Threshold*
drop (PPPoE Service Name Tables)

Syntax

drop;

Hierarchy Level

[edit protocols pppoe service-name-tables <table-name> service <service-name>],
[edit protocols pppoe service-name-tables <table-name> service <service-name> agent-specifier
aci <circuit-id-string> ari <remote-id-string>]

Release Information

Statement introduced in Junos OS Release 10.0.
Support at [edit protocols pppoe service-name-tables <table-name> service <service-name>
agent-specifier aci <circuit-id-string> ari <remote-id-string>] hierarchy level introduced in Junos
OS Release 10.2.

Description

Direct the router to drop (ignore) a PPPoE Active Discovery Initiation (PADI) control
packet received from a PPPoE client that contains the specified service name tag or
agent circuit identifier/agent remote identifier (ACI/ARI) information. This action
effectively denies the client's request to provide the specified service, or to accept requests
from the subscriber or subscribers represented by the ACI/ARI information.

Required Privilege

Level

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

Related Documentation

• Configuring PPPoE Service Name Tables
**drop-timeout**

**Syntax**

drop-timeout milliseconds;

**Hierarchy Level**

[edit interfaces interface-name mlfr-uni-nni-bundle-options],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For link services, multilink, and voice services interfaces only, configure the drop timeout period, in milliseconds.

**Options**

milliseconds—Drop timeout period.

- **Range:** 0 through 2000 milliseconds
- **Default:** 0 ms (disabled)

**Required Privilege**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Junos OS Services Interfaces Library for Routing Devices
ds0-options

Syntax

ds0-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  byte-encoding (nx56 | nx64);
  fcs (16 | 32);
  idle-cycle-flag (flags | ones);
  invert-data;
  loopback payload;
  start-end-flag (filler | shared);
}

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure DS0-specific physical interface properties.

The remaining statements are explained separately. See CLI Explorer.

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

Related Documentation
• Configuring Channelized DS3-to-DS0 Interfaces
**dsl-options**

**Syntax**

dsl-options {
    loopback local;
    operating-mode mode;
}

**Hierarchy Level**
[edit interfaces at-fpc/pic/port]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For J Series Services Routers only, modify the properties of the digital subscriber line for an ATM interface.

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**
- [ATM-over-ADSL Overview](#)
- [Junos OS Interfaces and Routing Configuration Guide](#)
**dsr**

**Syntax**

```
 dsr (ignore | normal | require);
```

**Hierarchy Level**

```
 [edit interfaces interface-name serial-options dce-options],
 [edit interfaces interface-name serial-options dte-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For EIA-530 and V.35 interfaces only, configure the from-DCE signal, data-set-ready (DSR).

**Options**

- **ignore**—The from-DCE signal is ignored.
- **normal**—Normal DSR signal handling as defined by the TIA/EIA Standard 530.
- **require**—The from-DCE signal must be asserted.

Default: normal

**Required Privilege Level**

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

**Related Documentation**

- Configuring the Serial Signal Handling on page 324
**dsr-polarity**

Syntax  
dsr-polarity (negative | positive);

Hierarchy Level  
[edit interfaces interface-name serial-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Configure DSR signal polarity.

Options  
**positive**—Positive signal polarity.

**negative**—Negative signal polarity.

Default: positive

Required Privilege Level  
interface—To view this statement in the configuration.

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

Related Documentation  
- Configuring Serial Signal Polarities on page 327
dte-options

Syntax

dte-options {
  control-signal (assert | de-assert | normal);
  cts (ignore | normal | require);
  dcd (ignore | normal | require);
  dsr (ignore | normal | require);
  dtr signal-handling-option;
  ignore-all;
  indication (ignore | normal | require);
  rts (assert | de-assert | normal);
  tm (ignore | normal | require);
}

Hierarchy Level  [edit interfaces interface-name serial-options]

Release Information  Statement introduced in Junos OS Release 8.3.
Statement previously known as control-leads.

Description  For M Series and T Series routers, configure the serial interface signal characteristics.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege  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 Serial Signal Handling on page 324
**dtr**

**Syntax**

```
dtr signal-handling-option;
```

**Hierarchy Level**

```
[edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For EIA-530 and V.35 interfaces only, configure the to-DCE signal, data-transmit-ready (DTR).

**Options**

- `signal-handling-option`—Signal handling for the DTR signal. The signal handling can be one of the following:
  - `assert`—The to-DCE signal must be asserted.
  - `auto-synchronize`—Normal DTR signal with automatic synchronization. This statement has two substatements:
    - `duration milliseconds`—Pulse duration of resynchronization.
      - **Range:** 1 through 1000 milliseconds
      - **Default:** 1000 milliseconds
    - `interval seconds`—Offset interval for resynchronization.
      - **Range:** 1 through 31 seconds
      - **Default:** 15 seconds
  - `de-assert`—The to-DCE signal must be deasserted.
  - `normal`—Normal DTR signal handling as defined by the TIA/EIA Standard 530.
    - **Default:** normal

**Required Privilege Level**

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

**Related Documentation**

- Configuring the Serial Signal Handling on page 324
**dtr-circuit**

**Syntax**

dtr-circuit (balanced | unbalanced);

**Hierarchy Level**

[edit interfaces interface-name serial-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For EIA-530 and V.35 interfaces only, configure a DTR circuit.

**Options**

balanced—Balanced DTR signal.

unbalanced—Unbalanced DTR signal.

Default: balanced

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

• Configuring the Serial DTR Circuit on page 327

**dtr-polarity**

**Syntax**


dtr-polarity (negative | positive);

**Hierarchy Level**

[edit interfaces interface-name serial-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure DTR signal polarity.

**Options**

positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

• Configuring Serial Signal Polarities on page 327
dump-on-flow-control

Syntax

dump-on-flow-control;

Hierarchy Level

[edit interfaces interface-name multiservice-options]

Release Information

Statement introduced in Junos OS Release 9.5.

Description

This option supports high availability functionality and can be used with various service interfaces, including rsp, rms, lsq, and rlsq.

Required Privilege

interface—To view this statement in the configuration.

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

Related Documentation

- Configuring Multiservice Physical Interface Properties on page 154
- Junos OS Services Interfaces Library for Routing Devices
- passive-monitor-mode on page 874
## dynamic-call-admission-control

### Syntax

```text
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
}
```

### Hierarchy Level

- `edit interfaces interface-name unit logical-unit-number`
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number`

### Release Information

Statement introduced in Junos OS Release 8.2.

### Description

(J4350 and J6350 Services Routers supporting voice over IP with the TGM550 media gateway module) For Fast Ethernet and Gigabit Ethernet interfaces, ISDN BRI interfaces, and serial interfaces with PPP or Frame Relay encapsulation, configure dynamic call admission control (CAC). Dynamic CAC provides enhanced control over WAN bandwidth. When dynamic CAC is configured on an interface responsible for providing call bandwidth, the TGM550 informs the Media Gateway Controller (MGC) of the bandwidth limit available for voice packets on the interface and requests the MGC to block new calls when the bandwidth is exhausted.

Dynamic CAC must be configured on each Services Router interface responsible for providing call bandwidth.

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 Dynamic Call Admission Control
- Junos OS Services Interfaces Library for Routing Devices
- Junos OS Interfaces and Routing Configuration Guide
**dynamic-profile (PPP)**

**Syntax**

dynamic-profile profile-name;

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number ppp-options]

**Release Information**

Statement introduced in Junos OS Release 9.5. Support for MLPPP on LSQ interfaces introduced in Junos OS Release 10.2.

**Description**

Specify the dynamic profile that is attached to the interface. On the MX Series routers, this statement is supported on PPPoE interfaces only.

**Required Privilege Level**

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

**Related Documentation**

- Dynamic Profiles Overview
- Configuring a Basic Dynamic Profile
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces
- Attaching Dynamic Profiles to MLPPP Bundles
- For hardware requirements, see Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces
**dynamic-profile (PPPoE Service Name Tables)**

**Syntax**

```
dynamic-profile profile-name;
```

**Hierarchy Level**

```
[edit protocols pppoe service-name-tables table-name service service-name],
[edit protocols pppoe service-name-tables table-name service-name service-name agent-specifier aci circuit-id-string ari remote-id-string]
```

**Release Information**

Statement introduced in Junos OS Release 10.2.

**Description**

Specify a dynamic profile to instantiate a dynamic PPPoE interface. You can associate a dynamic profile with a named service entry, empty service entry, or any service entry configured in a PPPoE service name table, or with an agent circuit identifier/agent remote identifier (ACI/ARI) pair defined for these services.

The dynamic profile associated with a service entry in a PPPoE service name table overrides the dynamic profile associated with the PPPoE underlying interface on which the dynamic PPPoE interface is created.

If you include the `dynamic-profile` statement at the `[edit protocols pppoe service-name-tables table-name service service-name service-name agent-specifier aci circuit-id-string ari remote-id-string]` hierarchy level, you cannot also include the `static-interface` statement at this level. The `dynamic-profile` and `static-interface` statements are mutually exclusive for ACI/ARI pair configurations.

**Options**

- `profile-name`—Name of the dynamic profile that the router uses to instantiate a dynamic PPPoE interface.

**Required Privilege Level**

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

**Related Documentation**

- Configuring PPPoE Service Name Tables
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
**dynamic-profile (Stacked VLAN)**

**Syntax**

```plaintext
dynamic-profile profile-name {
    accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
    access-profile vlan-dynamic-profile-name;
    ranges (any | low-tag–high-tag), (any | low-tag–high-tag);
}
```

**Hierarchy Level**

```
[edit interfaces interface-name auto-configure stacked-vlan-ranges]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

Configure a dynamic profile for use when configuring dynamic stacked VLANs.

**Options**

`profile-name`—Name of the dynamic profile that you want to use when configuring dynamic stacked VLANs.

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**

- Dynamic Profiles Overview
- Configuring a Basic Dynamic Profile
- Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs
**dynamic-profile (VLAN)**

**Syntax**

```bash
dynamic-profile profile-name {
    accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
    accept-out-of-band protocol;
    access-profile vlan-dynamic-profile-name;
    ranges (any | low-tag)–(any | high-tag);
}
```

**Hierarchy Level**

```
[edit interfaces interface-name auto-configure vlan-ranges]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

Configure a dynamic profile for use when configuring dynamic VLANs.

**Options**

- `profile-name`—Name of the dynamic profile that you want to use when configuring dynamic VLANs.

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**

- Dynamic Profiles Overview
- Configuring a Basic Dynamic Profile
- Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs
**dynamic-profiles**

**Syntax**

```plaintext
dynamic-profiles {
  profile-name {
    class-of-service {
      interfaces {
        interface-name ;
      }
      unit logical-unit-number {
        classifiers {
          type (classifier-name | default);
          output-traffic-control-profile (profile-name | $junos-cos-traffic-control-profile);
          report-ingress-shaping-rate bps;
          rewrite-rules {
            dscp (rewrite-name | default);
            dscp-ipv6 (rewrite-name | default);
            ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
            inet-precedence (rewrite-name | default);
          }
        }
      }
      scheduler-maps {
        map-name {
          forwarding-class class-name scheduler scheduler-name;
        }
      }
      schedulers {
        (scheduler-name) {
          buffer-size (seconds | percent percentage | remainder | temporal microseconds);
          drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol (any | non-tcp | tcp) drop-profile profile-name;
          excess-priority (low | high | $junos-cos-scheduler-excess-priority);
          excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
          overhead-accounting (shaping-mode) <bytes (byte-value)>;
          priority priority-level;
          shaping-rate (rate | predefined-variable);
          transmit-rate (percent percentage | rate | remainder) <exact | rate-limit>;
        }
      }
      traffic-control-profiles {
        profile-name {
          delay-buffer-rate (percent percentage | rate | $junos-cos-delay-buffer-rate);
          excess-rate (percent percentage | proportion value | percent $junos-cos-excess-rate);
          guaranteed-rate (percent percentage | rate | $junos-cos-guaranteed-rate);
          overhead-accounting (shaping-mode) <bytes (byte-value)>;
          scheduler-map map-name;
          shaping-rate (rate | predefined-variable);
        }
      }
      firewall {
        family {
          fast-update-filter filter-name {
```
interface-specific;
match-order [match-order];
term term-name {
  from {
    match-conditions;
  }
  then {
    action;
    action-modifiers;
  }
  only-at-create;
}
filter filter-name {
  enhanced-mode-override;
  fast-lookup-filter;
  instance-shared;
  interface-shared;
  interface-specific;
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
    only-at-create;
    filter filter-name {
      interface-specific;
      term term-name {
        from {
          match-conditions;
        }
        then {
          action;
          action-modifiers;
        }
      }
    }
  }
}
hierarchical-policer uid {
    aggregate {
        if-exceeding {
            bandwidth-limit limit bps;
            burst-size-limit bytes;
        }
        then {
            policer-action;
        }
    }
    premium {
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        then {
            policer-action;
        }
    }
    policer uid {
        filter-specific;
        if-exceeding {
            (bandwidth-limit bps | bandwidth-percent percentage);
            burst-size-limit bytes;
        }
        logical-bandwidth-policer;
        logical-interface-policer;
        physical-interface-policer;
        then {
            policer-action;
        }
    }
    three-color-policer uid {
        action {
            loss-priority high then discard;
        }
        logical-interface-policer;
        single-rate {
            (color-aware | color-blind);
            committed-burst-size bytes;
            committed-information-rate bps;
            excess-burst-size bytes;
        }
        two-rate {
            (color-aware | color-blind);
            committed-burst-size bytes;
            committed-information-rate bps;
            peak-burst-size bytes;
            peak-information-rate bps;
        }
    }
}
interfaces interface-name {
  interface-set interface-set-name {
    interface interface-name {
      unit logical unit number {
        advisory-options {
          downstream-rate rate;
          upstream-rate rate;
        }
      }
    }
  }
}

unit logical-unit-number {
  actual-transit-statistics;
  auto-configure {
    agent-circuit-identifier {
      dynamic-profile profile-name;
    }
    line-identity {
      include {
        accept-no-ids;
        circuit-id;
        remote-id;
      }
      dynamic-profile profile-name;
    }
  }
}

encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid |
  atm-tcc-vc-mux | atm-mippp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux |
  atm-snap | atm-tcc-snap | atm-vc-mux | ether-over-atm-llc |
  ether-vpls-over-atm-llc | ether-vpls-over-fr | ether-vpls-over-ppp | ethernet |
  frame-relay-ccc | frame-relay-ppp | frame-relay-tcc | frame-relay-ether-type |
  frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end | multilink-ppp |
  ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc | vlan-vci-ccc |
  vlan-tcc | vlan-vpl(s);

family family {
  address address;
  filter {
    adf {
      counter;
      input-precedence precedence;
      not-mandatory;
      output-precedence precedence;
      rule rule-value;
    }
    input filter-name {
      precedence precedence;
      shared-name filter-shared-name;
    }
    output filter-name {
      precedence precedence;
      shared-name filter-shared-name;
    }
  }
}

rpf-check {
  fail-filter filter-name;
}
mode loose;
}

service {
  input {
    service-set service-set-name {
      service-filter filter-name;
    }
    post-service-filter filter-name;
  }
  input-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (push | swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  output {
    service-set service-set-name {
      service-filter filter-name;
    }
  }
  output-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | swap);
    tag-protocol-id tpid;
    vlan-id number;
    pcef pcef-profile-name {
      activate rule-name | activate-all;
    }
  }
  unnumbered-address interface-name <preferred-source-address address>;
}

filter {
  input filter-name {
    shared-name filter-shared-name;
  }
  output filter-name {
    shared-name filter-shared-name;
  }
}

host-prefix-only;
ppp-options {
    aaa-options aaa-options-name;
    authentication [ authentication-protocols ];
    chap {
        challenge-length minimum minimum-length maximum maximum-length;
        local-name name;
    }  
    ignore-magic-number-mismatch;
    initiate-ncp (dual-stack-passive | ipv6 | ip)
    ipcp-suggest-dns-option;
    mru size;
    mtu (size | use-lower-layer);
    on-demand-ip-address;
    pap;
    peer-ip-address-optional;
    local-authentication {
        password password;
        username-include {
            circuit-id;
            delimiter character;
            domain-name name;
            mac-address;
            remote-id;
        }
    }
}
targeted-options {
    backup backup;
    group group;
    primary primary;
    weight ($junos-interface-target-weight | weight-value);
}
telemetry {
    subscriber-statistics;
    queue-statistics {
        interface $junos-interface-name {
            refresh rate;
            queues queue set;
        }
        interface-set $junos-interface-set-name {
            refresh rate;
            queues queue set;
        }
    }
}
}
}
}
}
vlan-id number;
vlan-tags outer [tpid],vlan-id [inner [tpid],vlan-id];
}
}
}
interfaces {
    demux0 {...}
}
}
}

Interfaces Fundamentals for Routing Devices
policy-options {
  prefix-list uid {
    ip-addresses;
    dynamic-db;
  }
}
predefined-variable-defaults predefined-variable <variable-option> default-value;
profile-type remote-device-service;
protocols {
  igmp {
    interface interface-name {
      accounting;
      disable;
      group-limit limit;
      group-policy;
      group-threshold value;
      immediate-leave
      log-interval seconds;
      no-accounting;
      oif-map;
      passive;
      promiscuous-mode;
      ssm-map ssm-map-name;
      ssm-map-policy ssm-map-policy-name
      static {
        group group {
          source source;
        }
      }
      version version;
    }
  }
  mld {
    interface interface-name {
      (accounting | no-accounting);
      disable;
      group-limit limit;
      group-policy;
      group-threshold value;
      immediate-leave;
      log-interval seconds;
      oif-map;
      passive;
      ssm-map ssm-map-name;
      ssm-map-policy ssm-map-policy-name;
      static {
        group multicast-group-address {
          exclude;
          group-count number;
          group-increment increment;
          source ip-address {
            source-count number;
            source-increment increment;
          }
        }
      }
      version version;
    }
  }
  router-advertisement {
    interface interface-name {
      current-hop-limit number;
      default-lifetime seconds;
    }
  }
}
(managed-configuration | no-managed-configuration);
max-advertisement-interval seconds;
min-advertisement-interval seconds;
(other-stateful-configuration | no-other-stateful-configuration);
prefix prefix;
reachable-time milliseconds;
retransmit-timer milliseconds;
}
}
}

routing-instances routing-instance-name {
  interface interface-name;
  routing-options {
    access {
      route prefix {
        next-hop next-hop;
        metric route-cost;
        preference route-distance;
        tag route-tag;
        tag2 route-tag2;
      }
    }
    access-internal {
      route subscriber-ip-address {
        qualified-next-hop underlying-interface {
          mac-address address;
        }
      }
    }
    multicast {
      interface interface-name {
        no-qos-adjust;
      }
    }
  }
}

rib routing-table-name {
  access {
    route prefix {
      next-hop next-hop;
      metric route-cost;
      preference route-distance;
      tag route-tag;
      tag2 route-tag2;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
}
routing-options {
    access {
        route prefix {
            next-hop next-hop;
            metric route-cost;
            preference route-distance;
            tag route-tag;
            tag2 route-tag2;
        }
    }
    access-internal {
        route subscriber-ip-address {
            qualified-next-hop underlying-interface {
                mac-address address;
            }
        }
    }
    multicast {
        interface interface-name {
            no-qos-adjust;
        }
    }
    services {
        captive-portal-content-delivery {
            rule name {
                match-direction (input | input-output | output);
                term name {
                    then {
                        accept;
                        redirect url;
                        rewrite destination-address address <destination-port port-number>;
                        syslog;
                    }
                }
            }
        }
    }
    variables {
        variable-name {
            default-value default-value;
            equals expression;
            mandatory;
            uid;
            uid-reference;
        }
    }
}

Hierarchy Level   [edit]
Support at the filter, policer, hierarchical-policer, three-color-policer, and policy options hierarchy levels introduced in Junos OS Release 11.4.

Description  Create dynamic profiles for use with DHCP or PPP client access.

Options  profile-name—Name of the dynamic profile; string of up to 80 alphanumeric characters.

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
• Configuring a Basic Dynamic Profile
• Configuring Dynamic VLANs Based on Agent Circuit Identifier Information
• Dynamic Profiles for Subscriber Management
**e1-options**

Syntax

```plaintext
e1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
```

Hierarchy Level

[edit interfaces interface-name]

Release Information

Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description

Configure E1-specific physical interface properties.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege

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

Related Documentation

- Channelized E1 IQ and IQE Interfaces Overview
- Channelized STM1 Interfaces Overview
- E1 Interfaces Overview
- T1 Interfaces Overview
e3-options

Syntax

e3-options {
  atm-encapsulation (direct | pincp);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout feet;
  compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
  fcs (16 | 32);
  framing (g.751 | g.832);
  idle-cycle-flag value;
  invert-data;
  loopback (local | remote);
  (payload-scrambler | no-payload-scrambler);
  start-end-flag value;
  (unframed | no-unframed);
}

Hierarchy Level  [edit interfaces interface-name]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure E3-specific physical interface properties.

For ATM interfaces, you can configure a subset of E3 options statements.

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

- E3 Interfaces Overview
- T3 Interfaces Overview
- atm-options on page 430
east-interface

Syntax

east-interface [ 
node-id mac-address; 
control-channel channel-name { 
  vlan number; 
  interface name interface-name 
} 
interface-none 
  ring-protection-link-end; 
]

Hierarchy Level

[edit protocols protection-group ethernet-ring ring-name]

Release Information

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Define one of the two interface ports for Ethernet ring protection, the other being defined by the west-interface statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

EX Series switches do not use the node-id statement—the node ID is automatically configured on the switches using the MAC address.

NOTE: Always configure this port first, before configuring the west-interface statement.

NOTE: The Node ID is not configurable on EX Series switches. The node ID is automatically configured using the MAC address.

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

- Ethernet Ring Protection Switching Overview
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- west-interface on page 1147
 epsis-policer-overhead

Syntax  

egress-policer-overhead bytes;

Hierarchy Level  

[edit chassis fpc slot-number pic pic-number]

Release Information  

Statement introduced before Junos OS Release 11.1.

Description  

Add the specified number of bytes to the actual length of an Ethernet frame when determining the actions of Layer 2 policers, MAC policers, or queue rate limits applied to output traffic on the line card. You can configure egress policer overhead to account for egress shaping overhead bytes added to output traffic on the line card.

On M Series and T Series routers, this statement is supported on Gigabit Ethernet Intelligent Queuing 2 (IQ2) PICs and Enhanced IQ2 (IQ2E) PICs. On MX Series routers, this statement is supported for interfaces configured on Dense Port Concentrators (DPCs).

NOTE: This statement is not supported on Modular Interface Cards (MICs) or Modular Port Concentrators (MPCs) in MX Series routers.

Options  

bytes—Number of bytes added to a packet exiting an interface.  
Range: 0–255 bytes  
Default: 0

Required Privilege Level  

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

Related Documentation  

• egress-shaping-overhead  
• Policer Overhead to Account for Rate Shaping Overview  
• Example: Configuring Policer Overhead to Account for Rate Shaping  
• Configuring a Policer Overhead  
• CoS on Enhanced IQ2 PICs Overview
encapsulation (Container Interface)

Syntax
encapsulation (cisco-hdlc | ppp);

Hierarchy Level
[edit interfaces cin]

Release Information
Statement introduced in Junos OS Release 9.2.

Description
Container link-layer encapsulation type.

Options
cisco-hdlc—Use Cisco-compatible High-Level Data Link Control (HDLC) framing.
ppp—Use serial PPP encapsulation.

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

Related Documentation
• Displaying APS Using a Container Interface with ATM Encapsulation
• Configuring Container Interfaces for APS on SONET Links
encapsulation (Logical Interface)

Syntax

```
```

Hierarchy Level

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`
- `[edit interfaces rlsg number unit logical-unit-number]`
- `[edit protocols evpn]`

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (ether-net, vlan-ccc, and vlan-tcc options only).
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers. Only the `atm-ccc-cell-relay` and `atm-ccc-vc-mux` options are supported on ACX Series routers.
Statement introduced in Junos OS Release 17.3R1 for QFX10000 Series switches (ether-net-ccc and vlan-ccc options only).

Description

Configure a logical link-layer encapsulation type. Not all encapsulation types are supported on the switches. See the switch CLI.

Options

- **atm-ccc-cell-relay**—Use ATM cell-relay encapsulation.
  - **atm-ccc-vc-mux**—Use ATM virtual circuit (VC) multiplex encapsulation on CCC circuits. When you use this encapsulation type, you can configure the `ccc` family only.
  - **atm-cisco-nlpid**—Use Cisco ATM network layer protocol identifier (NLPID) encapsulation. When you use this encapsulation type, you can configure the `inet` family only.
  - **atm-mlppp-llc**—For ATM2 IQ interfaces only, use Multilink Point-to-Point (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services or Voice Services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.
  - **atm-nlpid**—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the `inet` family only.
  - **atm-ppp-llc**—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over AAL5 LLC encapsulation.
atm-ppp-vc-mux—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over ATM AAL5 multiplex encapsulation.

atm-snap—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM subnetwork attachment point (SNAP) encapsulation.

atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.

atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the tcc family only.

atm-vc-mux—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the inet family only.

ether-over-atm-llc—(All IP interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) For interfaces that carry IP traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

ether-vpls-over-fr—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, per RFC 2427, Multiprotocol Interconnect over Frame Relay.

NOTE: The SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and the DS3/E3 MIC do not support Ethernet over Frame Relay encapsulation.

ether-vpls-over-ppp—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Point-to-Point Protocol (PPP) encapsulation to support Bridged Ethernet over PPP-encapsulated TDM interfaces for VPLS applications.

ethernet—Use Ethernet II encapsulation (as described in RFC 894, A Standard for the Transmission of IP Datagrams over Ethernet Networks).

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces.
ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.

NOTE: The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

ethernet-vpls-fr—Use in a VPLS setup when a CE device is connected to a PE router over a time-division multiplexing (TDM) link. This encapsulation type enables the PE router to terminate the outer layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the ccc family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the ppp family only.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the tcc family only.

gre-fragmentation—For adaptive services interfaces only, use GRE fragmentation encapsulation to enable fragmentation of IPv4 packets in GRE tunnels. This encapsulation clears the do not fragment (DF) bit in the packet header. If the packet’s size exceeds the tunnel’s maximum transmission unit (MTU) value, the packet is fragmented before encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

multilink-ppp—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—Use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with MPCs.
**ppp-over-ether-over-atm-llc**—(MX Series routers with MPCs using the ATM MIC with SFP only) For underlying ATM interfaces, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

**vlan-bridge**—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible-ethernet-services, and bridging enabled and that must accept packets carrying TPID 0xb100 or a user-defined TPID.

**vlan-ccc**—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-vci-ccc**—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-tcc**—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

**vlan-vpls**—Use Ethernet VLAN encapsulation on VPLS circuits.

**vxlan**—Use VXLAN data plane encapsulation for EVPN.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Layer 2 Switching Cross-Connects Using CCC
- Configuring the Encapsulation for Layer 2 Switching TCCs
- Configuring Interface Encapsulation on Logical Interfaces on page 173
- Configuring the CCC Encapsulation for LSP Tunnel Cross-Connects
- Circuit and Translational Cross-Connects Overview on page 255
- Identifying the Access Concentrator
- Configuring ATM Interface Encapsulation
- Configuring VLAN and Extended VLAN Encapsulation
- Configuring ATM-to-Ethernet Interworking on page 262
- Configuring Interface Encapsulation on PTX Series Packet Transport Routers on page 117
- Configuring CCC Encapsulation for Layer 2 VPNs
- Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits
- Configuring ATM for Subscriber Access
- Understanding CoS on ATM IMA Pseudowire Interfaces Overview
- Configuring Policing on an ATM IMA Pseudowire
**encapsulation**

**List of Syntax**

Syntax for Physical Interfaces: M Series, MX Series, QFX Series, T Series, PTX Series on page 571
Syntax for Physical Interfaces: SRX Series on page 571
Syntax for Logical Interfaces: SRX Series on page 571

Syntax for Physical Interfaces: M Series, MX Series, QFX Series, T Series, PTX Series


Syntax for Physical Interfaces: SRX Series


Syntax for Logical Interfaces: SRX Series

encapsulation ( dix | ether-vpls-fr | frame-relay-ppp | ppp-over-ether | vlan-bridge | vlan-ccc | vlan-tcc | vlan-vpls );

Physical Interfaces: M Series, MX Series, QFX Series, T Series, PTX Series

[edit interfaces interface-name],
[edit interfaces rlq number:number]

Logical Interfaces

[edit interfaces interface-name unit logical-unit-number ]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (flexible-ethernet-services, ethernet-ccc, and ethernet-tcc options only).

Description

For M Series, MX Series, QFX Series, T Series, PTX Series, specify the physical link-layer encapsulation type.

For SRX Series, specify logical link layer encapsulation.

NOTE: Not all encapsulation types are supported on the switches. See the switch CLI.
Default   **ppp**—Use serial PPP encapsulation.
Physical Interface Options and Logical Interface Options

For physical interfaces:

NOTE: Frame Relay, ATM, PPP, SONET, and SATSOP options are not supported on EX Series switches.

- **atm-ccc-cell-relay**—Use ATM cell-relay encapsulation.

- **atm-pvc**—Defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*. When you configure physical ATM interfaces with ATM PVC encapsulation, an RFC 2684-compliant ATM Adaptation Layer 5 (AAL5) tunnel is set up to route the ATM cells over a Multiprotocol Label Switching (MPLS) path that is typically established between two MPLS-capable routers using the Label Distribution Protocol (LDP).

- **cisco-hdlc**—Use Cisco-compatible High-Level Data Link Control (HDLC) framing. E1, E3, SONET/SDH, T1, and T3 interfaces can use Cisco HDLC encapsulation. Two related versions are supported:
  - CCC version (**cisco-hdlc-ccc**)—The logical interface does not require an encapsulation statement. When you use this encapsulation type, you can configure the **ccc** family only.
  - TCC version (**cisco-hdlc-tcc**)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

- **cisco-hdlc-ccc**—Use Cisco-compatible HDLC framing on CCC circuits.

- **cisco-hdlc-tcc**—Use Cisco-compatible HDLC framing on TCC circuits for connecting different media.

- **ethernet-bridge**—Use Ethernet bridge encapsulation on Ethernet interfaces that have bridging enabled and that must accept all packets.

- **ethernet-over-atm**—For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces. As defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, this encapsulation type allows ATM interfaces to connect to devices that support only bridge protocol data units (BPDUs). Junos OS does not completely support bridging, but accepts BPU packets as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload, and drops the rest. For packets destined to the Ethernet LAN, a route lookup is done using the destination IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header, and the packet is forwarded to the ATM interface.

- **ethernet-tcc**—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC is not supported.
- **ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

- **ethernet-vpls-fr**—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

- **ethernet-vpls-ppp**—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 PPP connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use it to forward the packet into a given VPLS instance.

- **ether-vpls-over-atm-llc**—For ATM intelligent queuing (IQ) interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

- **extended-frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC. When you use this encapsulation type, you can configure the ccc family only.

- **extended-frame-relay-ether-type-tcc**—Use extended Frame Relay ether type TCC for Cisco-compatible Frame Relay for DLCIs 1 through 1022. This encapsulation type is used for circuits with different media on either side of the connection.

- **extended-frame-relay-tcc**—Use Frame Relay encapsulation on TCC circuits to connect different media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.

- **extended-vlan-bridge**—Use extended VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q VLAN tagging and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

- **extended-vlan-ccc**—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and 4-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values. Extended VLAN CCC encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. When you use this encapsulation type, you can configure the ccc family only. For 8-port, 12-port, and 48-port Fast Ethernet PICs, extended VLAN CCC is not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC is not supported.

- **extended-vlan-tcc**—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. For 4-port Gigabit Ethernet PICs, extended VLAN TCC is not supported.
• **extended-vlan-vpls**—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

```
NOTE: The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.
```

• **flexible-ethernet-services**—For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and for Gigabit Ethernet interfaces, use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. Aggregated Ethernet bundles can use this encapsulation type. This encryption type allows you to configure any combination of route, TCC, CCC, Layer 2 virtual private networks (VPNs), and VPLS encapsulations on a single physical port. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

• **flexible-frame-relay**—For IQ interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

• **frame-relay**—Use Frame Relay encapsulation is defined in RFC 1490, *Multiprotocol Interconnect over Frame Relay*. E1, E3, link services, SONET/SDH, T1, T3, and voice services interfaces can use Frame Relay encapsulation.

• **frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits. This encapsulation is same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC. The logical interface must also have **frame-relay-ccc** encapsulation. When you use this encapsulation type, you can configure the **ccc** family only.

• **frame-relay-ether-type**—Use Frame Relay ethernet type encapsulation for compatibility with the Cisco Frame Relay. IETF frame relay encapsulation identifies the payload format using NLPID and SNAP formats. Cisco-compatible Frame Relay encapsulation uses the Ethernet type to identify the type of payload.

```
NOTE: When the encapsulation type is set to Cisco-compatible Frame Relay encapsulation, ensure that the LMI type is set to ANSI or Q933-A.
```

• **frame-relay-ether-type-tcc**—Use Frame Relay ethernet type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media. This encapsulation is Cisco-compatible Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to TCC.
• **frame-relay-port-ccc**—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with Frame Relay transport. The connection between the two CE routers can be either user-to-network interface (UNI) or network-to-network interface (NNI); this is completely transparent to the PE routers. When you use this encapsulation type, you can configure the ccc family only.

• **frame-relay-tcc**—This encapsulation is similar to Frame Relay CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

• **generic-services**—Use generic services encapsulation for services with a hierarchical scheduler.

• **multilink-frame-relay-uni-nni**—Use MLFR UNI NNI encapsulation. This encapsulation is used on link services, voice services interfaces functioning as FRF.16 bundles, and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

• **ppp**—Use serial PPP encapsulation. This encapsulation is defined in RFC 1661, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*. PPP is the default encapsulation type for physical interfaces. E1, E3, SONET/SDH, T1, and T3 interfaces can use PPP encapsulation.

• **ppp-ccc**—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the ccc family only.

• **ppp-tcc**—Use serial PPP encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the tcc family only.

• **vlan-ccc**—Use Ethernet VLAN encapsulation on CCC circuits. VLAN CCC encapsulation supports TPID 0x8100 only. When you use this encapsulation type, you can configure the ccc family only.
• **vlan-vci-ccc**—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the ccc family only. All logical interfaces configured on the Ethernet interface must also have the encapsulation type set to vlan-vci-ccc.

• **vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

**NOTE:**
- Label-switched interfaces (LSIs) do not support VLAN VPLS encapsulation. Therefore, you can only use VLAN VPLS encapsulation on a PE-router-to-CE-router interface and not a core-facing interface.
- Starting with Junos OS release 13.3, a commit error occurs when you configure vlan-vpls encapsulation on a physical interface and configure family inet on one of the logical units. Previously, it was possible to commit this invalid configuration.

For logical interfaces:

• **frame-relay**—Configure a Frame Relay encapsulation when the physical interface has multiple logical units, and the units are either point to point or multipoint.

• **multilink-frame-relay-uni-nni**—Link services interfaces functioning as FRF.16 bundles can use Multilink Frame Relay UNI NNI encapsulation.

• **ppp**—For normal mode (when the device is using only one ISDN B-channel per call). Point-to-Point Protocol is for communication between two computers using a serial interface.

• **ppp-over-ether**—This encapsulation is used for underlying interfaces of pp0 interfaces.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Required Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
Related Documentation

- Understanding Physical Encapsulation on an Interface
- Configuring Interface Encapsulation on Physical Interfaces on page 114
- Configuring CCC Encapsulation for Layer 2 VPNs
- Configuring Layer 2 Switching Cross-Connects Using CCC
- Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits
- Configuring ATM Interface Encapsulation
- Configuring ATM-to-Ethernet Interworking on page 262
- Configuring VLAN and Extended VLAN Encapsulation
- Configuring VLAN and Extended VLAN Encapsulation
- Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces
- Configuring Interfaces for Layer 2 Circuits
- Configuring Interface Encapsulation on PTX Series Packet Transport Routers on page 117
- Configuring MPLS LSP Tunnel Cross-Connects Using CCC
- Configuring TCC
- Configuring VPLS Interface Encapsulation
- Configuring Interfaces for VPLS Routing
- Defining the Encapsulation for Switching Cross-Connects on page 257
- Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)
encoding

Syntax  encoding (nrz | nrzi);

Hierarchy Level  [edit interfaces interface-name serial-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For serial interfaces, set the line encoding format.

Default  The default line encoding is non-return to zero (NRZ).

Options  nrz—Use NRZ line encoding.

nrzi—Use non-return to zero inverted (NRZI) line encoding.

Required Privilege Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring Serial Line Encoding on page 330
**epd-threshold (Logical Interface)**

**Syntax**

```
epd-threshold cells plp1 cells;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address]
```

**Release Information**

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

**Description**

For ATM2 IQ interfaces only, define the early packet discard (EPD) threshold on a VC. The EPD threshold is a limit on the number of transmit packets that can be queued. Packets that exceed the limit are discarded. For interfaces configured in trunk mode, you can also configure dual EPD thresholds depending on the packet loss priorities (PLPs).

**Default**

Approximately 1 percent of the available cell buffers. If shaping is enabled, the default EPD threshold is proportional to the shaping rate according to the following formula:

```
default epd-threshold = number of buffers * shaping rate / line rate
```

The minimum EPD threshold value is 48 cells. If the default EPD threshold formula results in an EPD threshold of less than 48 cells, the result will be ignored, and the minimum value of 48 cells will be used.

**Options**

- **cells**—Maximum number of cells.
  
  **Range:** For 1-port and 2-port OC12 interfaces, 48 through 425,984 cells

**Required Privilege Level**

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

**Related Documentation**

- Configuring the ATM2 IQ EPD Threshold
- Configuring Two EPD Thresholds per Queue
epd-threshold (Physical Interface)

**Syntax**

```
epd-threshold cells plp1 cells;
```

**Hierarchy Level**

```
[edit interfaces at-fpc/pic/port atm-options scheduler-maps map-name forwarding-class class-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, define the EPD threshold on a VC. The EPD threshold is a limit on the number of transmit packets that can be queued. Packets that exceed the limit are discarded.

**Default**

If you do not include either the `epd-threshold` or the `linear-red-profile` statement in the forwarding class configuration, the Junos OS uses an EPD threshold based on the available bandwidth and other parameters.

**Options**

- **cells**—Maximum number of cells.
  - **Range:** For 1-port and 2-port OC12 interfaces, 48 through 425,984 cells. For 1-port OC48 interfaces, 48 through 425,984 cells. For 2-port OC3, DS3, and E3 interfaces, 48 through 212,992 cells. For 4-port DS3 and E3 interfaces, 48 through 106,496 cells.

  The `plp1` statement is 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 an ATM Scheduler Map
- `linear-red-profile` on page 733
es-options

**Syntax**

```
es-options {
  backup-interface interface-name;
}
```

**Hierarchy Level**

[edit interfaces es-fpc/pic/port]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

On ES interfaces, configure ES interface-specific interface properties.

The `backup-interface` statement is explained separately.

**Required Privilege Level**

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

**Related Documentation**

- *Junos OS Services Interfaces Library for Routing Devices*
ethernet (Protocols OAM)

List of Syntax

Syntax: MX, T, ACX Series Routers, SRX Firewalls, M320 and EX Series Switches
Syntax: EX Series Switches and NFX Series Devices on page 586

Syntax: MX, T, ACX Series Routers, SRX Firewalls, M320 and EX Series Switches

```
ethernet {
    connectivity-fault-management {
        action-profile profile-name {
            default-actions {
                interface-down;
            }
        }
    }
    performance-monitoring {
        delegate-server-processing;
        hardware-assisted-timestamping;
        hardware-assisted-keepalives;
        sla-iterator-profiles {
            profile-name {
                avg-fd-twoway-threshold;
                avg-ifdv-twoway-threshold;
                avg-flr-forward-threshold;
                avg-flr-backward-threshold;
                disable;
                calculation-weight {
                    delay delay-weight;
                    delay-variation delay-variation-weight;
                }
                cycle-time milliseconds;
                iteration-period connections;
                measurement-type (loss | statistical-frame-loss | two-way-delay);
            }
        }
    }
}
```

```
linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
}
```

```
maintenance-domain domain-name {
    level number;
    name-format (character-string | none | dns | mac+2octet);
    maintenance-association ma-name {
        short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
        protect-maintenance-association protect-ma-name;
        remote-maintenance-association remote-ma-name;
        continuity-check {
            convey-loss-threshold;
            hold-interval minutes;
            interface-status-tlv;
            interval (10m | 10s | 1m | 1s | 100ms);
            loss-threshold number;
            port-status-tlv;
        }
    }
}
```
mep mep-id {
  auto-discovery;
  direction (up | down);
  interface interface-name (protect | working);
  lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
    rem-err-xcon | xcon );
  priority number;
  remote-mep mep-id {
    action-profile profile-name;
    sla-iterator-profile profile-name {
      data-tlv-size size;
      iteration-count count-value;
      priority priority-value;
    }
  }
}
evcs evc-id {
  evc-protocol cfm management-domain domain-id (management-association 
    association-id) vpls (routing-instance instance-id);
  remote-uni-count count;
  multipoint-to-multipoint;
}
link-fault-management {
  action-profile profile-name {
    action {
      link-down;
      send-critical-event;
      syslog;
    }
    event {
      link-adjacency-loss;
      link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
      }
      protocol-down;
    }
  }
  interface interface-name {
    apply-action-profile;
    link-discovery {active | passive};
    loopback-tracking;
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    negotiation-options {
      allow-remote-loopback;
      no-allow-link-events;
    }
  }
  lmi {
    status-counter count;
    polling-verification-timer value;
    interface name {
      uni-id uni-name;
      status-counter number;
      polling-verification-timer value;
      evc-map-type {all-to-one-bundling | bundling | service-multiplexing};
      evc evc-name {
        default-vc;
        vlan-list vlan-id-list;
      }
    }
  }
}

Syntax: EX Series
Switches and NFX
Series Devices

ethernet {
  connectivity-fault-management {
    action-profile profile-name {
      action {
        interface-down;
      }
    }
    default-actions {
      interface-down;
    }
    event {
      adjacency-loss;
    }
  }
  esp-traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag (all | error | esp | interface | krt | lib | normal | task | timer);
  }
  linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
  }
  maintenance-association domain-name {
    level number;
    mip-half-function (none | default | explicit);
    name-format (character-string | none | dns | mac+2oct);
    maintenance-association ma-name {
      continuity-check {
        hold-interval minutes;
        interface-status-tlv;
        interval (10m | 10s | 1m | 1s | 100ms);
        loss-threshold number;
        port-status-tlv;
      }
      mep mep-id {
        auto-discovery;
        direction down;
        interface interface-name;
        priority
        remote-mep mep-id {
          action-profile profile-name;
          sla-iterator-profile profile-name {
            data-tlv-size size;
            iteration-count count-value;
            priority priority-value;
          }
        }
      }
      short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
    }
  }
  performance-monitoring {
    sla-iterator-profiles {
      profile-name {
        calculation-weight {
          
          Copyright © 2019, Juniper Networks, Inc.
      }}
    }
  }
}
delay delay-value;
delay-variation delay-variation-value;
}
cycle-time cycle-time-value;
iteration-period iteration-period-value;
measurement-type two-way-delay;
passive;
}
}
traceoptions {
  file filename <files number> <match regex> <size size> <world-readable |
  no-world-readable>;
  flag flag ;
  no-remote-trace;
}
}
link-fault-management {
  action-profile profile-name:
  action {
    syslog;
    link-down;
  }
  event {
    link-adjacency-loss;
    link-event-rate {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
  }
  interface interface-name {
    link-discovery (active | passive);
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    negotiation-options {
      allow-remote-loopback;
      no-allow-link-events;
    }
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
    no-world-readable>;
    flag flag ;
    no-remote-trace;
  }
}
Hierarchy Level: [edit protocols oam]

Release Information:
- Statement introduced in Junos OS Release 8.2 for MX, T, ACX Series routers, SRX firewalls, M320 and EX Series switches.
- Statement introduced in Junos OS Release 9.4 for EX Series switches and NFX Series devices.
- Connectivity-fault-management introduced in Junos OS Release 10.2 for EX Series switches.

Description:
Provide IEEE 802.3ah Operation, Administration, and Maintenance (OAM) support for Ethernet interfaces or configure connectivity fault management (CFM) for IEEE 802.1ag Operation, Administration, and Management (OAM) support.

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

Related Documentation:
- Enabling IEEE 802.3ah OAM Support
- Example: Configuring Ethernet OAM Link Fault Management
ethernet-policer-profile

Syntax

```
ethernet-policer-profile {
  input-priority-map {
    ieee802.1p premium [ values ];
  }
  output-priority-map {
    classifier {
      premium {
        forwarding-class class-name {
          loss-priority (high | low);
        }
      }
    }
  }
  policer cos-policer-name {
    aggregate {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    premium {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
  }
}
```

Hierarchy Level

- [edit interfaces interface-name gigether-options ethernet-switch-profile],
- [edit interfaces interface-name aggregated-ether-options ethernet-switch-profile]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

NOTE: On QFX Series standalone switches, this statement hierarchy is only supported on the Enhanced Layer 2 Switching CLI.

For Gigabit Ethernet IQ, 10-Gigabit Ethernet, Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and 100-Gigabit Ethernet Type 5 PIC with CFP, configure a class of service (CoS)-based policer. Policing applies to the inner VLAN identifiers, not to the outer tag. For Gigabit Ethernet interfaces with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), the premium policer is not supported.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

- Configuring Gigabit Ethernet Policers
ethernet-ring

Syntax

ethernet-ring ring-name {
  control-vlan (vlan-id | vlan-name);
  data-channel {
    vlan number
  }
  east-interface {
    control-channel channel-name {
      vlan number;
      interface name interface-name
    }
  }
guard-interval number;
node-id mac-address;
restore-interval number;
ring-protection-link-owner;
west-interface {
  control-channel channel-name {
    vlan number;
  }
}
}

Hierarchy Level
[edit protocols protection-group]

Release Information
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
For Ethernet PICs on MX Series routers or for EX Series switches, specify the Ethernet ring in an Ethernet ring protection switching configuration.

Options

ring-name—Name of the Ethernet protection ring.

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
• Ethernet Ring Protection Switching Overview
• Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
• Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
• Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
**ethernet-switch-profile**

**Syntax**
```
ethernet-switch-profile {
    ethernet-policer-profile {
        input-priority-map {
            ieee802.1p premium [values];
        }
        output-priority-map {
            classifier {
                premium {
                    forwarding-class class-name {
                        loss-priority (high | low);
                    }
                }
            }
        }
    }
    policer cos-policer-name {
        aggregate {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        premium {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
    }
    storm-control storm-control-profile;
    tag-protocol-id tpid;
    mac-learn-enable;
}
```

**Hierarchy Level**
- [edit interfaces interface-name gigether-options],
- [edit interfaces interface-name aggregated-ether-options],
- [edit interfaces interface-name aggregated-ether-options],
- [edit interfaces interface-name ether-options]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
- Statement introduced in Junos OS Release 13.2 for the QFX Series.
- Statement introduced in Junos OS Release 13.2X50-D15 for the EX Series switches.

**Description**

**NOTE:** On QFX Series standalone switches, the ethernet-policer-profile CLI hierarchy and the mac-learn-enable statement are supported only on the Enhanced Layer 2 Switching CLI.
For Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ2 and IQ2-E, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC, aggregated Ethernet with Gigabit Ethernet IQ interfaces, the built-in Gigabit Ethernet port on the M7i router); 100-Gigabit Ethernet Type 5 PIC with CFP; and Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces on EX Series switches, configure VLAN tag and MAC address accounting and filtering properties.

The remaining statements are explained separately. See CLI Explorer.

NOTE: When you gather interfaces into a bridge domain, the no-mac-learn-enable statement at the [edit interfaces interface-name gigether-options ethernet-switch-profile] hierarchy level is not supported. You must use the no-mac-learning statement at the [edit bridge-domains bridge-domain-name bridge-options interface interface-name] hierarchy level to disable MAC learning on an interface in a bridge domain. For information on disabling MAC learning for a bridge domain, see the MX Series Layer 2 Configuration Guide.

Default

If the ethernet-switch-profile statement is not configured, Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router) behave like Gigabit Ethernet interfaces.

Required Privilege Level

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

Related Documentation

- Configuring Gigabit Ethernet Policers
- Configuring MAC Address Filtering
- Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview
- Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
**eui-64**

**Syntax**  
eui-64;

**Hierarchy Level**  
[edit interfaces interface-name unit number family inet6 address address]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 12.2 for the QFX Series.  
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**  
For interfaces that carry IP version 6 (IPv6) traffic, automatically generate the host number portion of interface addresses.

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

**Related Documentation**  
- Configuring the Interface Address on page 191
evcs

Syntax  

```plaintext
evcs evc-id 
   evc-protocol cfm;
   remote-uni-count count;
   multipoint-to-multipoint;
}
```

Hierarchy Level  [edit protocols oam ethernet]

Release Information  Statement introduced in Junos OS Release 9.5.

Description  On MX Series routers with ge, xe, or ae interfaces, configure an OAM Ethernet virtual connection.

Options  

remote-uni-count count—(Optional) Specify the number of remote UNIs in the EVC configuration, the default is 1.

multipoint-to-multipoint—(Optional) Specify multiple points in the EVC configuration, the default is point-to-point if remote-uni-count is 1.

Remaining options 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 Ethernet Local Management Interface

• lmi (Ethernet OAM) on page 748
event (LFM)

List of Syntax  Syntax: MX, M, T, ACX Series Routers, SRX Firewalls and EX Series Switches on page 596
Syntax: EX Series Switches and NFX Series Devices on page 596

Syntax: MX, M, T, ACX Series Routers, SRX Firewalls and EX Series Switches

```plaintext
event {
    link-adjacency-loss;
    link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
    protocol-down;
}
```

Syntax: EX Series Switches and NFX Series Devices

```plaintext
event {
    link-adjacency-loss;
    link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
}
```

Hierarchy Level  [edit protocols oam ethernet link-fault-management action-profile]

Release Information  Statement introduced in Junos OS Release 8.5 for MX, M, T, ACX Series routers, SRX Series firewalls and EX Series switches.
Statement introduced in Junos OS Release 9.4 for EX Series switches and NFX devices.

Description  Configure link events in an action profile for Ethernet OAM link fault management (LFM).

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

Related Documentation  • Monitoring Protocol Status
• Configuring Ethernet OAM Link Fault Management
event-thresholds

Syntax

```plaintext
event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

Hierarchy Level

```plaintext
[edit protocols oam link-fault-management interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Configure threshold limit values for link events in periodic OAM PDUs.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Configuring Threshold Values for Local Fault Events on an Interface
fast-aps-switch

Syntax

```plaintext
fast-aps-switch;
```

Hierarchy Level

```plaintext
[edit interfaces interface-name sonet-options aps]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

(M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only, EX Series switches, and MX series routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only using container interfaces) Reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits.

NOTE:

- The fast APS switching feature is supported only within a single chassis on a MX series router using a container interface.
- Configuring this statement reduces the APS switchover time only when the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor is SAToP.
- When the `fast-aps-switch` statement is configured in revertive APS mode, you must configure an appropriate value for revert time to achieve reduction in APS switchover time.
- To prevent the logical interfaces in the data path from being shut down, configure appropriate hold-time values on all the interfaces in the data path that support TDM.
- The `fast-aps-switch` statement cannot be configured when the APS annex-b option is configured.
- The interfaces that have the `fast-aps-switch` statement configured cannot be used in virtual private LAN service (VPLS) environments.

Required Privilege Level

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

Related Documentation

- *Reducing APS Switchover Time in Layer 2 Circuits*
f-max-period

Syntax  
f-max-period number;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number]
[edit interfaces interface-name unit logical-unit-number rtp]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For all adaptive services interfaces and for ISDN interfaces on J Series Services Routers. Specify the maximum number of compressed packets allowed between the transmission of full headers in a compressed Real-Time Transport Protocol (RTP) traffic stream.

Options  
number—Maximum number of packets. The value can be from 1 through 65535.

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

Related Documentation  
• Configuring Bandwidth on Demand  
• Junos OS Services Interfaces Library for Routing Devices

facility-override

Syntax  
facility-override facility-name;

Hierarchy Level  
[edit interfaces interface-name services-options sysloghost hostname]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Override default facility for system log reporting.

Options  
facility-name—Name of facility that overrides the default assignment.

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

Related Documentation  
• Junos OS Services Interfaces Library for Routing Devices
failover-delay

Syntax  failover-delay milliseconds;

Hierarchy Level  [edit protocols vrrp]


Description  Configure the failover delay for VRRP and VRRP for IPv6 operations.

Options  milliseconds—Specify the failover delay time, in milliseconds.
  Range:  50 through 2000

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

Related Documentation  • Configuring VRRP and VRRP for IPv6
family (Dynamic Standard Interface)

Syntax

```
family family {
    access-concentrator name;
    address address;
    direct-connect;
    duplicate-protection;
    dynamic-profile profile-name;
    filter {
        adf {
            counter;
            input-precedence precedence;
            not-mandatory;
            output-precedence precedence;
            rule rule-value;
        }
        input filter-name {
            precedence precedence;
            shared-name filter-shared-name;
        }
        output filter-name {
            precedence precedence;
            shared-name filter-shared-name;
        }
    }
    input filter-name {
        precedence precedence;
        filter-shared-name;
    }
    output filter-name {
        precedence precedence;
        filter-shared-name;
    }
    mac-validate (loose | strict);
    max-sessions number;
    max-sessions-vsa-ignore;
    rpf-check {
        fail-filter filter-name;
        mode loose;
    }
    service {
        input {
            service-set service-set-name {
                service-filter filter-name;
            }
            post-service-filter filter-name;
        }
        output {
            service-set service-set-name {
                service-filter filter-name;
            }
        }
    }
    service-name-table table-name;
    short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max maximum-seconds> <filter [aci]>;
    unnumbered-address interface-name <preferred-source-address address>;
}
```

Hierarchy Level

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number]
```
**Release Information**  
Statement introduced in Junos OS Release 9.2.  
**pppoe** option added in Junos OS Release 11.2.

**Description**  
Configure protocol family information for the logical interface.

**NOTE:** Not all subordinate stanzas are available to every protocol family.

**Options**  
**family**—Protocol family:

- **inet**—IP version 4 suite
- **inet6**—IP version 6 suite
- **pppoe**—(MX Series routers with MPCs only) Point-to-Point Protocol over Ethernet
- **vpls**—Virtual private LAN service

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**

- [Static Routing on Logical Systems](#)
- [Configuring the Protocol Family on page 190](#)
family

Syntax

family family {
  accounting {
    destination-class-usage;
    source-class-usage {
      (input | output | input output);
    }
  }
  access-concentrator name;
  address address {
    ... the address subhierarchy appears after the main [edit interfaces interface-name unit logical-unit-number family family-name] hierarchy ...
  }
  bundle interface-name;
  core-facing;
  demux-destination {
    destination-prefix;
  }
  demux-source {
    source-prefix;
  }
  direct-connect;
  duplicate-protection;
  dynamic-profile profile-name;
  filter {
    group filter-group-number;
    input filter-name;
    input-list [ filter-names ];
    output filter-name;
    output-list [ filter-names ];
  }
  interface-mode (access | trunk);
  ipsec-sa sa-name;
  keep-address-and-control;
  mac-validate (loose | strict);
  max-sessions number;
  max-sessions-vasa-ignore;
  mtu bytes;
  multicast-only;
  nd6-stale-time seconds;
  negotiate-address;
  no-neighbor-learn;
  no-redirects;
  policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
  }
  primary;
  protocols [inet isompls];
  proxy inet-address address;
  receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name
    mode loose;
}
sampling {
    input;
    output;
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name < service-filter filter-name >;
    }
    output {
        service-set service-set-name < service-filter filter-name >;
    }
}
service-name-table table-name;
short-cycle-protection < lockout-time-min minimum-seconds lockout-time-max
    maximum-seconds > < filter [aci] >;
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [ number number-number ];
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    master-only;
    multipoint-destination address dci dlci-identifier;
    multipoint-destination address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate sustained rate);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    vrpl group-id {
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-key key key;
        authentication-type authentication;
        fast-interval milliseconds;
        (preempt | no-preempt) {
            hold-time seconds;
        }
        priority number;
        track {
            interface interface-name {
                bandwidth-threshold bits-per-second priority-cost priority;
                priority-cost priority;
            }
            priority-hold-time seconds;
            route prefix routing-instance instance-name priority-cost priority;
        }
    }
    virtual-address [ addresses ];
}
virtual-link-local-address ipv6-address;
}

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Configure protocol family information for the logical interface.</td>
</tr>
</tbody>
</table>

**NOTE:** Not all subordinate statements are available to every protocol family.
Options  

family—Protocol family:

- any—Protocol-independent family used for Layer 2 packet filtering

NOTE: This option is not supported on T4000 Type 5 FPCs.

- bridge—(M Series and T Series routers only) Configure only when the physical interface is configured with ethernet-bridge type encapsulation or when the logical interface is configured with vlan-bridge type encapsulation. You can optionally configure this protocol family for the logical interface on which you configure VPLS.

- ethernet-switching—(M Series and T Series routers only) Configure only when the physical interface is configured with ethernet-bridge type encapsulation or when the logical interface is configured with vlan-bridge type encapsulation

- ccc—Circuit cross-connect protocol suite. You can configure this protocol family for the logical interface of CCC physical interfaces. When you use this encapsulation type, you can configure the ccc family only.

- inet—Internet Protocol version 4 suite. You must configure this protocol family for the logical interface to support IP protocol traffic, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Internet Control Message Protocol (ICMP), and Internet Protocol Control Protocol (IPCP).


- iso—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite. You must configure this protocol family for the logical interface to support ISO-IS traffic.

- mlfr-end-to-end—Multilink Frame Relay FRF.15. You must configure this protocol or multilink Point-to-Point Protocol (MLPPP) for the logical interface to support multilink bundling.

- mlfr-uni-nni—Multilink Frame Relay FRF.16. You must configure this protocol or mlfr-end-to-end for the logical interface to support link services and voice services bundling.

- multilink-ppp—Multilink Point-to-Point Protocol. You must configure this protocol (or mlfr-end-to-end) for the logical interface to support multilink bundling.

- mpls—Multiprotocol Label Switching (MPLS). You must configure this protocol family for the logical interface to participate in an MPLS path.

- pppoe—Point-to-Point Protocol over Ethernet

- tcc—Translational cross-connect protocol suite. You can configure this protocol family for the logical interface of TCC physical interfaces.
• **tnp**—Trivial Network Protocol. This protocol is used to communicate between the Routing Engine and the router’s packet forwarding components. The Junos OS automatically configures this protocol family on the router’s internal interfaces only, as discussed in “Understanding Internal Ethernet Interfaces” on page 14.

• **vpls**—(M Series and T Series routers only) Virtual private LAN service. You can optionally configure this protocol family for the logical interface on which you configure VPLS. VPLS provides an Ethernet-based point-to-multipoint Layer 2 VPN to connect customer edge (CE) routers across an MPLS backbone. When you configure a VPLS encapsulation type, the family vpls statement is assumed by default.

MX Series routers support dynamic profiles for VPLS pseudowires, VLAN identifier translation, and automatic bridge domain configuration.

For more information about VPLS, see the *Junos OS VPNs Library for Routing Devices*.

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 Protocol Family on page 190](#)
fastether-options

Syntax

```
fastether-options {
  802.3ad {
    ae [x (primary | backup);
    lacp {
      port-priority;
    }
  }
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  ingress-rate-limit rate;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
}
```

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure Fast Ethernet-specific interface properties.

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
- Ethernet Interfaces Overview
**fcs**

**Syntax**
```
fcs (16 | 32);
```

**Hierarchy Level**
```
[edit interfaces e1-fpc/pic/port],
[edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name sonet-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**
For E1/E3, SONET/SDH, and T1/T3 interfaces, configure the frame checksum (FCS) on the interface. The checksum must be the same on both ends of the interface.

On a channelized OC12 interface, the SONET/SDH fcs statement is not supported. To configure FCS on each DS3 channel, you must include the t3-options fcs statement in the configuration for each channel. For SONET/SDH, the channelized OC12 interface supports DS3 to STS-1 to OC12. For SDH, the channelized OC12 interface supports NxDS3 to NxVC3 to AU3 to STM.

**NOTE:** When configuring E1 or T1 interfaces on 10-port Channelized E1/T1 I奎 PICs, the fcs statement must be included at the [edit interfaces e1-fpc/pic/port] or [edit interfaces t1-fpc/pic/port] hierarchy level as appropriate.

**Options**
16—Use a 16-bit frame checksum on the interface.
32—Use a 32-bit frame checksum on the interface. Using a 32-bit checksum provides more reliable packet verification, but some older equipment might not support 32-bit checksums.

**Default:** 16

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

**Related Documentation**
- Configuring the E1 Frame Checksum
- Configuring the E3 Frame Checksum
- Configuring the SONET/SDH Frame Checksum
feac-loop-respond

Syntax (feac-loop-respond | no-feac-loop-respond);

Hierarchy Level [edit interfaces interface-name t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For T3 interfaces only, configure the router so a remote CSU can place the local router into loopback.

If you configure remote or local loopback with the T3 loopback statement, the router does not respond to FEAC requests from the CSU even if you include the feac-loop-respond statement in the configuration. For the router to respond, you must delete the loopback statement from the configuration.

You must rollback the setting done on the remote CSU prior to deactivating the feac-loop-respond statement. If the remote CSU cannot comply, clear the remote loop through local configuration to achieve the cleanup. For example, configure remote loopback on the interface and then delete the remote loopback.

Default The router does not respond to FEAC requests.

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

Related Documentation

• Configuring the T3 FEAC Response
• loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3) on page 760
• remote-loopback-respond on page 955
**fec** (gigether)

**Syntax**  
`fec (fec91 | none)`

**Hierarchy Level**  
`[edit interfaces interface-name gigether-options]`

**Release Information**  
Statement introduced in Junos OS Release 16.1R1  
Statement introduced in Junos OS Release 16.1X65D30 for PTX1000 routers  
Statement introduced in Junos OS Release 17.1R1 for PTX5000 routers  
Statement introduced in Junos OS Release 17.3R1 for MX10003 routers  
Statement introduced in Junos OS Release 17.4R1 for MX204 routers

**Description**  
(MX Series Routers with MPC7E, MPC8E, and MPC9E, MX10003 Router with MX10003 MPC, MX204 Router, PTX1000, FPC3-PTX-U2 and FPC3-PTX-U3 on PTX5000) Enable or disable RS-FEC (Reed-Solomon Forward Error Correction) for a 100-Gigabit Ethernet interface. By default, the Junos OS software enables or disables forward error correction based on the plugged-in optics. For instance, Junos OS software enables RS-FEC for 100G SR4 optics and disables RS-FEC for 100G LR4 optics.

This statement allows you to override the default behavior and explicitly enable or disable RS-FEC. For instance, you can extend the reach of 100G LR4 optics when you explicitly enable RS-FEC for the optics. RS-FEC is compliant with IEEE 802.3-2015 Clause 91.

Once you enable or disable RS-FEC using this statement, this behavior applies to any 100-Gigabit Ethernet optical transceiver installed in the port associated with the interface.

**NOTE:** FPC-PTX-P1-A and FPC2-PTX-P1A on PTX5000 routers do not support RS-FEC.

FPC3-SFF-PTX-1H and FP3-SFF-PTX-1T with PE-10-U-QSFP28 PIC and LR4 optics on PTX3000 and PTX5000 routers supports RS-FEC only on port 2. For PE-10-U-QSFP28 with LR4 optics, RS-FEC is the default FEC mode on port 2 and NONE is the default FEC mode on ports 0,1,3 through 9. For PE-10-U-QSFP28 with SR4 optics, RS-FEC is enabled by default on all ports. Do not modify the FEC mode on any port irrespective of the optics installed.

**Default**  
Junos OS software automatically enables or disables RS-FEC based on the type of pluggable optics used.

**Options**  
- **fec91**—Enables RS-FEC. RS-FEC is compliant with IEEE 802.3-2015 Clause 91.
- **none**—Disables RS-FEC.
Required Privilege Level

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

Related Documentation

- MPC7E (Multi-Rate) on MX Series Routers Overview
- MPC8E on MX Series Routers Overview
- MPC9E on MX Series Routers Overview
- Determining Transceiver Support for the PTX1000
filter

Syntax

```
filter {
  group filter-group-number;
  input filter-name;
  input-list [ filter-names ];
  output filter-name;
  output-list [ filter-names ];
}
```

Hierarchy Level

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

Release Information

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

Description

NOTE: On EX Series switches, the group, input-list, output-filter statements are not supported under the [edit interfaces interface-name unit logical-unit-number family family], [edit interfaces interface-name unit logical-unit-number family inet], [edit interfaces interface-name unit logical-unit-number family inet6], and [edit interfaces interface-name unit logical-unit-number family mpls] hierarchies.

Apply a filter to an interface. You can also use filters for encrypted traffic. When you configure filters, you can configure them under the family ethernet-switching, inet, inet6, mpls, or vpls only.

Options

- `group filter-group-number`—Define an interface to be part of a filter group. The default filter group number is 0.
  - Range: 0 through 255
- `input filter-name`—Name of one filter to evaluate when packets are received on the interface.
- `output filter-name`—Name of one filter to evaluate when packets are transmitted on the interface.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Applying a Filter to an Interface on page 220
• Junos OS Administration Library
• Configuring Gigabit Ethernet Interfaces (CLI Procedure)
• Configuring Firewall Filters (CLI Procedure)
• family
filter (Applying to an Interface)

Syntax

```
filter {
  input filter-name;
  output filter-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Apply a filter to an interface. You can also use filters for encrypted traffic. When you configure filters, you can configure the family `inet`, `inet6`, `mpls`, or `vpls` only.

**NOTE:** Mpls firewall filters applied on output interface are not supported on PTX10003 router due to product limitation.

Options

- **input filter-name**—Name of one filter to evaluate when packets are received on the interface.
- **output filter-name**—Name of one filter to evaluate when packets are transmitted on the interface.

Required Privilege Level

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

Related Documentation

- `simple-filter`
- **Configuring and Applying Tricolor Marking Policers**
- **Example: Classifying Packets Based on Their Destination Address**
- **Example: Configuring and Verifying a Complex Multifield Filter**
- **Example: Writing Different DSCP and EXP Values in MPLS-Tagged IP Packets**
- **Configuring a Simple Filter**
- **Configuring Policers Based on Logical Interface Bandwidth**
- **Effect of Two-Color Policers on Shaping Rate Changes**
**flexible-vlan-tagging**

**Syntax**
```
flexible-vlan-tagging;
```

**Hierarchy Level**
- [edit interfaces ae]
- [edit interfaces ge-fpc/pic/port]
- [edit interfaces et-fpc/pic/port]
- [edit interfaces ps0]
- [edit interfaces xe-fpc/pic/port]

**Release Information**
- Statement introduced in Junos OS Release 8.1.
- Support for aggregated Ethernet added in Junos OS Release 9.0.
- Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
- Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
- Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

**Description**
Support simultaneous transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port, and on pseudowire logical interfaces.

This statement is supported on M Series and T Series routers, for Fast Ethernet and Gigabit Ethernet interfaces only on Gigabit Ethernet IQ2 and IQ2-E, IQ, and IQE PICs, and for aggregated Ethernet interfaces with member links in IQ2, IQ2-E, and IQ PICs or in MX Series DPCs, or on Ethernet interfaces for PTX Series Packet Transport Routers or 100-Gigabit Ethernet Type 5 PIC with CFP.

This statement is supported on Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces on EX Series and QFX Series switches.

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

**Related Documentation**
- Enabling VLAN Tagging
- Configuring Flexible VLAN Tagging on PTX Series Packet Transport Routers
- Configuring Double-Tagged VLANs on Layer 3 Logical Interfaces
flow-control

**Syntax**

(flow-control | no-flow-control);

**Hierarchy Level**

[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options],
[edit interfaces interface-name multiservice-options],
[edit interfaces interface-range name aggregated-ether-options],
[edit interfaces interface-range name ether-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 in EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

**Description**

For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the router or switch to the remote side of the connection. Enabling flow control is useful when the remote device is a Gigabit Ethernet switch. Flow control is not supported on the 4-port Fast Ethernet PIC.

**NOTE:** On the Type 5 FPC, to prioritize control packets in case of ingress oversubscription, you must ensure that the neighboring peers support MAC flow control. If the peers do not support MAC flow control, then you must disable flow control.

**Default**

Flow control is enabled.

**NOTE:** Flow control is enabled by default only on physical interfaces and it is disabled by default on aggregated Ethernet interfaces.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Flow Control
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support
 flow-control-options

Syntax

```
flow-control-options {
  down-on-flow-control;
  dump-on-flow-control;
  reset-on-flow-control;
  up-on-flow-control;
}
```

Hierarchy Level

```
[edit interfaces mo-fpc/pic/port multiservice-options]
```

Release Information

Statement introduced before Junos OS Release 8.4.

Description

Configure the flow control options for application recovery in case of a prolonged flow control failure.

- **down-on-flow-control**—Bring interface down during prolonged flow control.

- **dump-on-flow-control**—Cause core dump during prolonged flow control.

**NOTE:** Starting with Junos OS Release 15.1, on MX Series routers with MS-MICs and MS-MPCs, instead of an eJunos kernel core file, the multiservices PIC management daemon (mspmand) core file is generated when a prolonged flow control failure occurs and when you configure the setting to generate a core dump during prolonged flow control (by using the dump-on-flow-control option with the flow-control-options statement). The watchdog functionality continues to generate a kernel core file in such scenarios.

- **reset-on-flow-control**—Reset interface during prolonged flow control.

**NOTE:** Starting in Junos OS Release 16.1R7, the reset-on-flow-control option has no effect on the MS-MIC, MS-MPC, MS-DPC, MS-PIC 100, MS-PIC 400, and MS-PIC 500 line cards. This is because starting in Release 16.1R7, Junos OS restarts these line cards to recover them from stuck state due to prolonged flow control.

- **up-on-flow-control**—Cause interface to remain in stuck state until you manually restart the PICs.

**NOTE:** Starting in Junos OS Release 16.1R7, if interfaces on an MS-PIC or MS-DPC are in stuck state because of prolonged flow control, Junos OS restarts the service PICs to recover them from this state. However, if you
want the PICs to remain in stuck state until you manually restart the PICs, configure the up-on-flow-control option. In releases before Release 16.1R7, there is no action taken to recover service PICs from this state unless one of the options for the flow-control-options statement is configured, or service PIC is manually restarted.


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

force

Syntax  force (protect | working);

Hierarchy Level  [edit interfaces interface-name sonet-options aps ]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Perform a forced switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch. It can be overridden by a signal failure on the protect circuit, thus causing a switch to the working circuit.

Options  protect—Request the circuit to become the protect circuit.
working—Request the circuit to become the working circuit.

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

Related Documentation  • Configuring Switching Between the Working and Protect Circuits
• request on page 957
forward-and-send-to-re

Syntax forward-and-send-to-re;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet targeted-broadcast], [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet targeted-broadcast]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify that IP packets destined for a Layer 3 broadcast address be forwarded to an egress interface and the Routing Engine. The packets are broadcast only if the egress interface is a LAN interface.

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

Related Documentation • Configuring Targeted Broadcast on page 251
• targeted-broadcast on page 1044
• Understanding Targeted Broadcast on page 250
**forwarding-class (ATM2 IQ Scheduler Maps)**

Syntax

```
forwarding-class class-name {
  epd-threshold cells plp1 cells;
  linear-red-profile profile-name;
  priority (high | low);
  transmit-weight (cells number | percent number);
}
```

Hierarchy Level  
[edit interfaces at-fpc/pic/port atm-options scheduler-maps map-name]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For ATM2 IQ interfaces only, define forwarding class name and option values.

Options

- **class-name**—Name of forwarding class.

  The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- [ATM2 IQ VC Tunnel CoS Components Overview](#)
- [Applying Scheduler Maps to ATM Interfaces](#)
forwarding-class (Gigabit Ethernet IQ Classifier)

Syntax

```
forwarding-class class-name {
    loss-priority (high | low);
}
```

Hierarchy Level

[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier premium]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For Gigabit Ethernet IQ interfaces only, define forwarding class name and option values.

Options

- `class-name`—Name of forwarding class.
  
  The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Specifying an Output Priority Map
- input-priority-map on page 682
- forwarding-class statement in the Class of Service Feature Guide (Routers and EX9200 Switches)
**forward-only**

**Syntax**  
`forward-only;`

**Hierarchy Level**  
```
[edit interfaces interface-name unit logical-unit-number family inet targeted-broadcast],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet targeted-broadcast]
```

**Release Information**  
Statement introduced in Junos OS Release 10.2.

**Description**  
Specify that IP packets destined for a Layer 3 broadcast address be forwarded to an egress interface only. The packets are broadcast only if the egress interface is a LAN interface.

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

**Related Documentation**  
- Configuring Targeted Broadcast on page 251
- `targeted-broadcast on page 1044`
- Understanding Targeted Broadcast on page 250
fragment-threshold

Syntax
fragment-threshold bytes;

Hierarchy Level
[edit interfaces interface-name m1fr-uni-nni-bundle-options],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For multilink, link services, and voice services interfaces, set the fragmentation threshold.

Options
bytes—Maximum size, in bytes, for multilink packet fragments. Any nonzero value must be a multiple of 64 bytes.
Range: 128 through 16,320 bytes
Default: 0 bytes (no fragmentation)

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

Related Documentation
- Junos OS Services Interfaces Library for Routing Devices
**frame-error**

**Syntax**  
frame-error count;

**Hierarchy Level**  
[edit protocols oam ethernet link-fault-management action-profile event link-event-rate],  
[edit protocols oam link-fault-management interface interface-name event-thresholds]

**Release Information**  
Statement introduced in Junos OS Release 8.4.

**Description**  
Threshold for sending frame error events or taking the action specified in the action profile.

A frame error is any frame error on the underlying physical layer. The threshold is reached when the number of frame errors reaches the configured value within the window.

The window or period during which frame errors are counted is 5 seconds or multiples of it (with a maximum value of 1 minute). This window denotes the duration as intervals of 100 milliseconds, encoded as a 16-bit unsigned integer. This window is not configurable in Junos OS. According to the IEEE 802.3ah standard, the default value of the frame-errors window is 1 second. This window has a lower bound of 1 second and an upper bound of 1 minute.

**Options**  
- **count**—Threshold count for frame error events.  
  
  **Range:** 0 through 100

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

**Related Documentation**  
- Configuring Threshold Values for Local Fault Events on an Interface  
- Configuring Threshold Values for Fault Events in an Action Profile
### frame-period

**Syntax**  
frame-period count;

**Hierarchy Level**  
[edit protocols oam ethernet link-fault-management action-profile event link-event-rate],  
[edit protocols oam link-fault-management interface interface-name event-thresholds]

**Release Information**  
Statement introduced in Junos OS Release 8.4.

**Description**  
Threshold for sending frame period error events or taking the action specified in the action profile.

A frame error is any frame error on the underlying physical layer. The frame period threshold is reached when the number of frame errors reaches the configured value within the period window. The default period window is the number of minimum-size frames that can be transmitted on the underlying physical layer in 1 second. The window is not configurable.

**Options**  
- **count**—Threshold count for frame period error events.  
  **Range:** 0 through 100

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

**Related Documentation**  
- Configuring Threshold Values for Local Fault Events on an Interface  
- Configuring Threshold Values for Fault Events in an Action Profile
frame-period-summary

Syntax

frame-period-summary count;

Hierarchy Level

[edit protocols oam ethernet link-fault-management action-profile event link-event-rate],
[edit protocols oam link-fault-management interface interface-name event-thresholds]

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Threshold for sending frame period summary error events or taking the action specified in the action profile.

An errored frame second is any 1-second period that has at least one errored frame. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period window. The default window is 60 seconds. The window is not configurable.

Options

count—Threshold count for frame period summary error events.

Range: 0 through 100

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring Threshold Values for Local Fault Events on an Interface
• Configuring Threshold Values for Fault Events in an Action Profile
framing (E1, E3, and T1 Interfaces)

Syntax
framing (g704 | g704-no-crc4 | g.751 | g.832 | unframed | sf | esf);

Hierarchy Level
[edit interfaces ce1-fpc/pic/port],
[edit interfaces ct1-fpc/pic/port],
[edit interfaces at-fpc/pic/port e3-options],
[edit interfaces e1-fpc/pic/port e1-options],
[edit interfaces t1-fpc/pic/port t1-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description
Configure the framing format.

NOTE: When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the framing statement must be included at the [edit interfaces ce1-fpc/pic/port] or [edit interfaces ct1-fpc/pic/port] hierarchy level as appropriate.

Default
esf for T1 interfaces; g704 for E1 interfaces. There is no default value for E3 over ATM interfaces.

Options
esf—Extended superframe (ESF) mode for T1 interfaces.
g704—G.704 framing format for E1 interfaces.
g704-no-crc4—G.704 framing with no cyclic redundancy check 4 (CRC4) for E1 interfaces.
g.751—G.751 framing format for E3 over ATM interfaces.
g.832—G.832 framing format for E3 over ATM interfaces.
sf—Superframe (SF) mode for T1 interfaces.
unframed—Unframed mode for E1 interfaces.

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

Related Documentation
- Configuring E1 Framing
- Configuring E3 and T3 Parameters on ATM Interfaces
- Configuring T1 Framing
framing (10-Gigabit Ethernet Interfaces)

Syntax

framing (lan-phy | wan-phy);  
precise-bandwidth;

Hierarchy Level

[edit interfaces xe-fpc/pic/port]

[edit interfaces et-fpc/pic/port] (PTX Series Packet Transport Routers and MX Series Routers)

Release Information

Statement introduced in Junos OS Release 8.0.  
Statement introduced in Junos OS Release 12.3R2 for PTX Series Packet Transport Routers.  
The option precise-bandwidth introduced in Junos OS Release 19.3R1 for MX Series Routers.

Description

For routers supporting the 10-Gigabit Ethernet interface, configure the framing format.  
WAN PHY mode is supported on MX240, MX480, MX960, T640, T1600, T4000, and PTX Series Packet Transport Routers routers only.

NOTE:

• The T4000 Core Router supports only LAN PHY mode in Junos OS Release 12.1R1.  
Starting with Junos OS Release 12.1R2, WAN PHY mode is supported on the T4000 routers with the 12-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (PF-12XGE-SFPP).  
Starting with Junos OS Release 12.2, WAN PHY mode is supported on the T4000 routers with the 24-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (PF-24XGE-SFPP).

• On PTX Series routers, WAN PHY mode is supported only on the 24-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+.

• When the PHY mode changes, interface traffic is disrupted because of port reinitialization.

• In Junos OS Releases 17.4R2, 17.4R3, and later, on the following MPCs or routers, you cannot configure wan-phy mode at 10-Gbps, 40-Gbps, and 100-Gbps on a per-port basis:

  • MPC7E-10G, MPC7E-MRATE, MX2K-MPC8E, and MX2K-MPC9E
  • MPC10003
  • MX204 router
  • JNP10K-LC2101 MPC

Default

Operates in LAN PHY mode.
Options

lan-phy—10GBASE-R interface framing format that bypasses the WIS sublayer to directly stream block-encoded Ethernet frames on a 10-Gigabit Ethernet serial interface.

wan-phy—10GBASE-W interface framing format that allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and SONET devices.

precise-bandwidth—Enables precise bandwidth for WAN-PHY interface framing format.

Required Privilege Level

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

Related Documentation

• Framing Overview
• Configuring SONET Options for 10-Gigabit Ethernet Interfaces

framing (SONET and SDH Interfaces)

Syntax

framing (sdh | sonet);

Hierarchy Level

[edit interfaces so-fpc/pic/port]

Release Information

Statement introduced in Junos OS Release 8.1.

Description

This functionality allows you to mix SONET and SDH modes on interfaces on the same PIC.

• For the 4-port OC48 PIC with SFP installed and the 4-port OC192 PIC in T Series and M Series routers, configure SONET or SDH framing on a per-port basis.

• For 1-port OC192/STM64 MICs with XFP on MX Series routers, configure the SONET or SDH framing on the single port.

Default

Default framing mode is SONET.

Options

sdh—SDH framing.

sonet—SONET framing.

Required Privilege Level

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

Related Documentation

• Configuring SONET/SDH Framing Mode for Ports
gigether-options

Syntax

gigether-options {
  802.3ad {
    ae (primary | backup);
    lacp {
      port-priority;
    }
  }
  ctle;
  pre-emphasis;
  differential-amplitude;
  (asynchronous-notification | no-asynchronous-notification);
  (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online | local-interface-offline>;
  fec {
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    (loopback | no-loopback);
  }
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  no-auto-mdix
  source-address-filter {
    mac-address;
  } (source-filtering | no-source-filtering);
  speed ethernet-switch-profile {
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ];
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [ values ];
      }
      output-priority-map {
        classifier {
          premium {
            forwarding-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
    }
    cos-policer-name {
      aggregate {
        bandwidth-limit bps;
        burst-size-limit bytes;
      }
      premium {
        bandwidth-limit bps;
      }
    }
  }

burst-size-limit bytes;
}
}
}
}
}

Hierarchy Level  [edit interfaces interface-name]

Release Information  Statement introduced before Junos OS Release 7.4. Options ctle, pre-emphasis and differential-amplitude introduced in Junos OS Release 19.3R1 for QFX5200 line of switches.

Description  Configure Gigabit Ethernet specific interface properties.

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  • Ethernet Interfaces Overview
                      • gigether-options (ACX Series)
**gratuitous-arp-reply**

**Syntax**

```
(gratuitous-arp-reply | no-gratuitous-arp-reply);
```

**Hierarchy Level**

```
[edit interfaces interface-name]
[edit interfaces interface-range interface-range-name]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 in EX Series switches.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

**Description**

For Ethernet interfaces, enable updating of the Address Resolution Protocol (ARP) cache for gratuitous ARPs.

**Default**

Updating of the ARP cache is disabled on all Ethernet interfaces.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Gratuitous ARP
- no-gratuitous-arp-request on page 831
guard-interval

Syntax  
guard-interval number;

Hierarchy Level  
[edit protocols protection-group ethernet-ring ring-name]

Release Information  
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description  
When a link goes down, the ring protection link (RPL) activates. When the downed link comes back up, the RPL link receives notification, restores the link, and waits for the restore interval before issuing another block on the same link. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

Options  
number—Guard timer interval, in milliseconds.
Range: 10 through 2000 ms
Default: 500 ms

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

Related Documentation  
- Ethernet Ring Protection Switching Overview
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
- Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
hardware-assisted-timestamping

Syntax

hardware-assisted-timestamping;

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management performance-monitoring]

Release Information

Statement introduced in Junos OS Release 9.5.

Description

For Ethernet interfaces on Enhanced and Enhanced Queuing Dense Port Concentrators (DPCs) in MX Series routers only, enable hardware-assisted timestamping support for Ethernet frame delay measurement.

By default, the ETH-DM feature calculates frame delays using software-based timestamping of the ETH-DM PDU frames sent and received by the MEPs in the session. As an option that can increase the accuracy of ETH-DM calculations when the DPC is loaded with heavy traffic in the receive direction, you can enable hardware-assisted timestamping of session frames in the receive direction.

Required Privilege

Level

interface—To view this statement in the configuration.

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

Related Documentation

• Ethernet Frame Delay Measurements Overview

• Guidelines for Configuring Routers to Support an ETH-DM Session

• Enabling the Hardware-Assisted Timestamping Option
**Syntax**

`high-plp-threshold percent;`

**Hierarchy Level**

`[edit interfaces at-fpc pic/port atm-options linear-red-profiles profile-name]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, define CoS VC drop profile fill-level percentage when linear RED is applied to cells with high PLP. When the fill level exceeds the defined percentage, packets with high PLP are randomly dropped by RED. This statement is mandatory.

**Options**

`percent`—Fill-level percentage when linear RED is applied to cells with PLP.

**Required Privilege Level**

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

**Related Documentation**

- ATM2 IQ VC Tunnel CoS Components Overview
- `high-plp-max-threshold` on page 641
  - `low-plp-max-threshold` on page 767
  - `low-plp-threshold` on page 768
  - `queue-depth` on page 937
**hello-timer**

**Syntax**  
hello-timer milliseconds;

**Hierarchy Level**  
[edit interfaces *interface-name* mlfr-uni-NNI-bundle-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For link services and voice services interfaces only, configure the rate at which hello messages are sent. A hello message is transmitted after a period defined in milliseconds has elapsed.

**Options**  
milliseconds—The rate at which hello messages are sent.  
**Range:** 1 through 180 milliseconds  
**Default:** 10 milliseconds

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

**Related Documentation**  
- Junos OS Services Interfaces Library for Routing Devices  
- acknowledge-timer on page 399  
- address on page 407
hierarchical-policer

**Syntax**

```
hierarchical-policer name
aggregate {
  if-exceeding {
    bandwidth-limit bandwidth;
    burst-size-limit burst;
  }
  then {
    discard;
  }
}
```

```
premium {
  if-exceeding {
    bandwidth-limit bandwidth;
    burst-size-limit burst;
  }
  then {
    discard;
  }
}
```

**Hierarchy Level**

[edit firewall]

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, specify a hierarchical policer.

**Options**

Options are described separately.

**Required Privilege**

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

**Related Documentation**

- Applying Policers on page 210
- Class of Service Feature Guide (Routers and EX9200 Switches)
hierarchical-scheduler (Subscriber Interfaces on MX Series Routers)

Syntax
hierarchical-scheduler {
  implicit-hierarchy;
  maximum-hierarchy-levels number;
}

Hierarchy Level [edit interfaces interface-name]

Release Information
Statement introduced in Junos OS Release 10.1.
  Support on GRE tunnel interfaces configured on physical interfaces on MICs or MPCs in
  MX Series routers added in Junos OS Release 13.3.
  Support for up to four hierarchy levels added in Junos OS Release 16.1.

Description
Configure hierarchical scheduling options on the interface.

The statement is supported on the following interfaces:

- MIC and MPC interfaces in MX Series routers
- GRE tunnel interfaces configured on physical interfaces hosted on MIC or MPC line
  cards in MX Series routers

To enable hierarchical scheduling on MX Series routers, configure the
hierarchical-scheduler statement at each member physical interface level of a particular
aggregated Ethernet interface as well as at that aggregated Ethernet interface level. On
other routing platforms, it is enough if you include this statement at the aggregated
Ethernet interface level.

Options
  implicit-hierarchy—Configure four-level hierarchical scheduling. When you include the
  implicit-hierarchy option, a hierarchical relationship is formed between the CoS
  scheduler nodes at level 1, level 2, level 3, and level 4. The implicit-hierarchy option
  is supported only on MPC/MIC subscriber interfaces and interface sets on MX Series
  routers.

  maximum-hierarchy-levels number—Specify the maximum number of hierarchical
  scheduling levels allowed for node scaling, from 2 through 4 levels. The default
  number of levels is 3. The maximum-hierarchy-levels option is supported on MPC/MIC
  or EQ DPC subscriber interfaces and interface sets on MX Series routers.

  • If you set maximum-hierarchy-levels to 2, interface sets are not allowed. In this case,
    if you configure a level 2 interface set, you generate Packet Forwarding Engine errors.

  • If you do not include the maximum-hierarchy-levels option, keeping the default number
    of hierarchy levels at 3, interface sets can be at either level 2 or level 3, depending on
    whether the member logical interfaces within the interface set have a traffic control
    profile. If any member logical interface has a traffic control profile, then the interface
set is a level 2 CoS scheduler node. If no member logical interface has a traffic control profile, the interface set is at level 3.

---

**CAUTION:** MPC3E, 32x10GE MPC4E, and 2x100GE + 8x10GE MPC4E MPCs support only two levels of scheduling hierarchy. When enabling hierarchical scheduling on these cards, you must explicitly set maximum-hierarchy-levels to 2.

---

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

**Related Documentation**
- Understanding Hierarchical CoS for Subscriber Interfaces
- Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links
- Configuring Hierarchical Schedulers for CoS
- Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface
- Hierarchical CoS on MPLS Pseudowire Subscriber Interfaces Overview

---

**high-plp-max-threshold**

**Syntax**
```
high-plp-max-threshold percent;
```

**Hierarchy Level**
```
[edit interfaces at-fpc/pic/port atm-options linear-red-profiles profile-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For ATM2 IQ interfaces only, define the drop profile fill-level for the high PLP CoS VC. When the fill level exceeds the defined percentage, all packets are dropped.

**Options**
- **percent**—Fill-level percentage when linear random early discard (RED) is applied to cells with PLP.

---

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

**Related Documentation**
- ATM2 IQ VC Tunnel CoS Components Overview
- low-plp-max-threshold on page 767
- low-plp-threshold on page 768
- queue-depth on page 937
**high-plp-threshold**

**Syntax**

```
high-plp-threshold percent;
```

**Hierarchy Level**

```
[edit interfaces at-fpc/pic/port atm-options linear-red-profiles profile-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, define CoS VC drop profile fill-level percentage when linear RED is applied to cells with high PLP. When the fill level exceeds the defined percentage, packets with high PLP are randomly dropped by RED. This statement is mandatory.

**Options**

`percent`—Fill-level percentage when linear RED is applied to cells with PLP.

**Required Privilege Level**

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

**Related Documentation**

- *ATM2 IQ VC Tunnel CoS Components Overview*
  - high-plp-max-threshold on page 641
  - low-plp-max-threshold on page 767
  - low-plp-threshold on page 768
  - queue-depth on page 937
**hold-interval (OAM)**

**Syntax**

```
hold-interval minutes;
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name continuity-check]
```

**Release Information**

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

**Description**

The time to wait in minutes before flushing the maintenance association end point (MEP) database, if no updates occur. The configurable range is 1 minute through 30240 minutes. The default value is 10 minutes.

---

**NOTE:** Hold timer based flushing is applicable only for auto discovered remote MEPs and not for statically configured remote MEPs.

---

**Options**

- `minutes`—Time to wait, in minutes.

**Required Privilege Level**

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

**Related Documentation**

- *Continuity Check Protocol Parameters Overview*
- *Configuring Continuity Check Protocol Parameters for Fault Detection*
**hold-interval (Protection Group)**

**Syntax**

```plaintext
hold-interval number;
```

**Hierarchy Level**

```plaintext
[edit protocols protection-group ethernet-ring name]
```

**Release Information**

Statement introduced in Junos OS Release 9.4.

**Description**

Specify the hold-off timer interval for all rings in 100 millisecond (ms) increments.

**Options**

- **number**—Hold-timer interval, in milliseconds.
  - **Range:** 0 through 10,000 ms
  - **Default:** 100 ms

**Required Privilege Level**

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

**Related Documentation**

- *Ethernet Ring Protection Switching Overview*
- *Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*
**hold-time (APS)**

**Syntax**

```
hold-time milliseconds;
```

**Hierarchy Level**

```
[edit interfaces interface-name sonet-options aps]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Hold-time value to use to determine whether a neighbor APS router is operational.

**Options**

- `milliseconds`—Hold-time value.
  - **Range:** 1 through 65,534 milliseconds
  - **Default:** 3000 milliseconds (3 times the advertisement interval)

**Required Privilege**

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

**Related Documentation**

- Configuring APS Timers
- advertise-interval on page 409
hold-time (Physical Interface)

Syntax

hold-time up milliseconds down milliseconds;

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-range interface-range-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 10.4R5 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Statement introduced in Junos OS Release 12.1 for the SRX Series.

Description

Specify the hold-time value to use to damp shorter interface transitions milliseconds. The hold timer enables interface damping by not advertising interface transitions until the hold timer duration has passed. When a hold-down timer is configured and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still down, then the router begins to advertise the interface as being down. Similarly, when a hold-up timer is configured and an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still up, then the router begins to advertise the interface as being up.

NOTE:

- We recommend that you configure the hold-time value after determining an appropriate value by performing repeated tests in the actual hardware environment. This is because the appropriate value for hold-time depends on the hardware (XFP, SFP, SR, ER, or LR) used in the networking environment.
- The hold-time option is not available for controller interfaces.

NOTE: On MX Series routers with MPC3E and MPC4E, we recommend that you do not configure the hold-down timer to be less than 1 second. On MX Series routers with MPC5EQ-100G10G (MPC5EQ) or MPC6E (MX2K-MPC6E) with 100-Gigabit Ethernet MIC with CFP2 OTN interfaces, we recommend that you do not configure the hold-down timer to be less than 3 seconds.

Default

Interface transitions are not damped.
Options

**down milliseconds**—Hold time to use when an interface transitions from up to down. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

**Range:** 0 through 4,294,967,295

**Default:** 0 (interface transitions are not damped)

**up milliseconds**—Hold time to use when an interface transitions from down to up. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

**Range:** 0 through 4,294,967,295

**Default:** 0 (interface transitions are not damped)

**Required Privilege Level**

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

**Related Documentation**

- advertise-interval on page 409
- interfaces (EX Series switches)
  - Physical Interface Damping Overview on page 143
  - Damping Shorter Physical Interface Transitions on page 149
  - Damping Longer Physical Interface Transitions on page 150
hold-time (SONET/SDH Defect Triggers)

Syntax       hold-time up milliseconds down milliseconds;

Hierarchy Level  [edit interfaces interface-name sonet-options trigger defect]

Release Information Statement introduced before Junos OS Release 7.4.

Description  For ATM over SONET/SDH and SONET/SDH interfaces only, apply up and down hold times to SONET/SDH defect triggers. When you apply a down hold time to a defect, the defect must remain present for at least the hold-time period before the interface is marked down. When you apply an up hold time to a defect, the defect must remain absent for at least the hold-time period before the interface is marked up, assuming no other defect is outstanding.

**NOTE:**

- When up or down hold times are applied to SONET defect triggers of a 10-Gigabit Ethernet WAN-PHY interface, only the defects generated in the WAN Interface Sublayer (WIS) are damped. Therefore, if the hold times are applied to SONET defect triggers only, a 10-Gigabit Ethernet WAN-PHY interface might be marked up or down because of the faults that are generated in other layers, such as the Physical Coding Sublayer (PCS) or Physical Medium Attachment Sublayer (PMA), 10 Gigabit Media Independent Interface (XGMII) Extender Sublayer (XGXS), and Media Access Control (MAC). To damp the interface up or down events of a 10-Gigabit Ethernet WAN-PHY interface, you need to apply up or down hold-times for the interface at the [edit interfaces interface-name] hierarchy level.

- On M Series and T Series platforms with Channelized SONET IQ PICs and Channelized SONET IQE PICs, the SONET defect alarm trigger hold-time statement is not supported.

Default  If you do not include this statement, when a defect is detected the interface is marked down immediately, and when the defect becomes absent the interface is marked up immediately.

Options  

- **down milliseconds**—Hold time to wait before the interface is marked down.  
  **Range:** 1 through 65,534 milliseconds  
  **Default:** No hold time

- **up milliseconds**—Hold time to wait before the interface is marked up.
Range: 1 through 65,534 milliseconds
Default: No hold time

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

Related Documentation
• Configuring SONET/SDH Defect Triggers
• hold-time (Physical Interface) on page 646

host (Interfaces)

Syntax
host hostname {
  services severity-level;
  facility-override facility-name;
  log-prefix prefix-value;
  port port-number;
}

Hierarchy Level
[edit interfaces interface-name services-options syslog]

Release Information
Statement introduced before Junos OS Release 7.4.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.

Description
Specify the hostname for the system logging utility.
Starting with Junos OS release 17.4R1, you can configure up to a maximum of four system log servers (combination of local system log hosts and remote system log collectors) for each service set for ms interface under [edit interfaces interface-name services-options] hierarchy.

Options
hostname—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.

From Junos OS Release 17.4R1, you can configure up to four system log hosts.
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
• Applying Filters and Services to Interfaces
**host-prefix-only**

**Syntax**  
host-prefix-only;

**Hierarchy Level**  
- [edit dynamic-profiles interfaces interface-name unit logical-unit-number],
- [edit interfaces interface-name unit logical-unit-number],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],
- [edit logical-systems logical-system-name routing-instances routing-instance-name interfaces interface-name unit logical-unit-number]

**Release Information**  
Statement introduced in Junos OS Release 17.2 on MX Series routers.

**Description**  
(MPC5 and MPC6 cards) Improve datapath performance by allowing only DHCPv4 subscribers that negotiate a 32-bit prefix to come up on the underlying VLAN interface. All DHCP subscribers on the underlying interface must negotiate a 32-bit prefix. Subscribers that negotiate a subnet prefix are not brought up. You can configure this statement for static or dynamic subscribers.

**NOTE:** You must add or remove this statement before subscribers become active. The configuration fails if you attempt to configure the statement while subscribers are active.

**NOTE:** You must also configure demux-source inet for the logical interface. Only inet is supported. A commit error occurs if you specify demux-source inet6 or demux-source [inet inet6].

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

**Related Documentation**  
- Configuring an IP Demultiplexing Interface on page 296
- Configuring a VLAN Demultiplexing Interface on page 301
iccp

Syntax
iccp [ traceoptions; { file <filename> <files number> <match regular-expression> <microsecond-stamp> <size size> <world-readable | no-world-readable>; flag flag; no-remote-trace; } local-ip-address ip address; session-establishment-hold-time value; authentication-key string; peer ip-address [ local-ip-address ip address; session-establishment-hold-time value; authentication-key string; redundancy-group-id-list redundancy-group-id-list; liveness-detection; ] ]

Hierarchy Level
[edit protocols iccp]
[edit logical-systems logical-system-name protocols iccp]

Release Information

Description
Configure Interchassis Control Protocol (ICCP) between the multichassis link aggregation group (MC-LAG) peers. ICCP replicates forwarding information, validates configurations, and propagates the operational state of the MC-LAG members.

Default
If you do not include this statement, no ICCP protocol tracing operations are performed.

Options
traceoptions—Set Interchassis Control Protocol (ICCP) tracing options.

local-ip-address—Specify the source address where the ICCP packet is routed.

session-establishment-hold-time—Specify if the chassis takes over as the master at the ICCP session.

authentication-key—Specify TCP Message Digest 5 (MD5) option for an ICCP TCP session.

peer ip-address—Specify the IP address of the peer that hosts an MC-LAG. You must configure ICCP for both peers that host the MC-LAG.

redundancy-group-id-list—Specify the redundancy groups between two ICCP peers.

liveness-detection—Specify Bidirectional Forwarding Detection (BFD) protocol options.
<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring ICCP for MC-LAG on page 198
idle-cycle-flag

Syntax idle-cycle-flag value;

Hierarchy Level
[edit interfaces e1-fpc/pic/port],
[edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name serial-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description Configure the value that the DS0, E1, E3, T1, or T3 interface transmits during idle cycles.

NOTE: When configuring E1 or T1 interfaces on 10-port Channelized E1/T1 IQE PICs, the idle-cycle-flag statement must be included at the [edit interfaces e1-fpc/pic/port] or [edit interfaces t1-fpc/pic/port] hierarchy level as appropriate.

Options value—Value to transmit in the idle cycles:

- flags—Transmit the value 0x7E.
- ones—Transmit the value 0xFF (all ones).

Default: Flags

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

Related Documentation
- Configuring the E1 Idle Cycle Flag
- Configuring the E3 Idle Cycle Flag
- Configuring the T1 Idle Cycle Flag
- Configuring the T3 Idle Cycle Flag
idle-timeout

Syntax  idle-timeout seconds;

Hierarchy Level  [edit interfaces dln unit logical-unit-number dialer-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  On J Series Services Routers with ISDN interfaces, configure the number of seconds the link is idle before losing connectivity.

Options  seconds—Time for which the connection can remain idle. For interfaces configured to use a filter for traffic, the idle timeout is based on traffic.

Range: 1 through 429497295
Default: 120 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 Interfaces and Routing Configuration Guide
**IEEE802.1p**

**Syntax**
```
ieee802.1p premium [ values ];
```

**Hierarchy Level**
```
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile input-priority-map]
[edit interfaces interface-name ether-options ethernet-switch-profile ethernet-policer-profile input-priority-map]
```

**Release Information**
- Statement introduced before Junos Release 7.4.
- Statement introduced in Junos OS Release 13.2 for the QFX Series.

**Description**
For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, configure premium priority values for IEEE 802.1p input traffic.

**Options**
- **values**—Define IEEE 802.1p priority values to be treated as premium.
  - **Range:** 0 through 7

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

**Related Documentation**
- *Specifying an Input Priority Map*
if-exceeding (Hierarchical Policer)

Syntax

```plaintext
if-exceeding {
    bandwidth-limit bps;
    burst-size-limit bytes;
}
```

Hierarchy Level

- [edit dynamic-profiles profile-name firewall hierarchical-policer aggregate],
- [edit dynamic-profiles profile-name firewall hierarchical-policer premium],
- [edit firewall hierarchical-policer aggregate],
- [edit firewall hierarchical-policer premium]

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the [edit dynamic-profiles ... aggregate] and [edit dynamic-profiles ... premium] hierarchy level introduced in Junos OS Release 11.4.

Description

For M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, T4000 routers with Type 5 FPC and Enhanced Scaling Type 4 FPC, specify bandwidth and burst limits for a premium or aggregate component of a hierarchical policer.

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

Related Documentation

- [Hierarchical Policer Configuration Overview](#)
- [Hierarchical Policers](#)
- [aggregate (Hierarchical Policer)](#)
- [bandwidth-limit (Hierarchical Policer)](#) on page 442
- [burst-size-limit (Hierarchical Policer)](#) on page 455
- [hierarchical-policer](#)
- [premium (Hierarchical Policer)](#) on page 918
if-exceeding-pps (Hierarchical Policer)

Syntax

if-exceeding-pps {
    pps-limit pps;
    packet-burst packets;
}

Hierarchy Level

[edit dynamic-profiles profile-name firewall hierarchical-policer hierarchical-policer-name aggregate],
[edit dynamic-profiles profile-name firewall hierarchical-policer hierarchical-policer-name premium],
[edit firewall hierarchical-policer hierarchical-policer-name aggregate],
[edit firewall hierarchical-policer hierarchical-policer-name premium]

Release Information

Statement introduced in Junos OS Release 15.2 for MX Series routers with MPCs.

Description

For MX Series routers, if-exceeding-pps allows you to configure a packets-per-second (pps)-based trigger for a premium or aggregate component of a hierarchical policer. When applied to the loopback interface (lo0), this kind of trigger can help protect the Routing Engine from DDoS attacks. When applied in other areas, to either transit or control traffic, it is a more fine-grained monitor.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

• Hierarchical Policer Configuration Overview
• Hierarchical Policers
• aggregate (Hierarchical Policer)
• bandwidth-limit (Hierarchical Policer) on page 442
• burst-size-limit (Hierarchical Policer) on page 455
• hierarchical-policer
• premium (Hierarchical Policer) on page 918
igmp-snooping

List of Syntax

Syntax (EX Series and NFX Series) on page 658
Syntax (MX Series) on page 658
Syntax (QFX Series) on page 660
Syntax (SRX Series) on page 661

Syntax (EX Series and NFX Series)

igmp-snooping {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match
    regex>;
    flag flag (detail | disable | receive | send);
  }
  vlan (vlan-name | all) {
    data-forwarding {
      receiver {
        install;
        mode (proxy | transparent);
        (source-list | source-vlans) vlan-list;
        translate;
      }
      source {
        groups group-prefix;
      }
    }
    disable;
    immediate-leave;
    interface interface-name {
      group-limit limit;
      host-only-interface;
      immediate-leave;
      multicast-router-interface;
      static {
        group multicast-ip-address;
      }
    }
    (l2-querier | igmp-querier (QFabric Systems only)) {
      source-address ip-address;
    }
    proxy {
      source-address ip-address;
    }
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count number;
    version number;
  }
}

Syntax (MX Series)

igmp-snooping {


immediate-leave;
interface interface-name {
    group-limit limit;
    host-only-interface;
    immediate-leave;
    multicast-router-interface;
    static {
        group ip-address {
            source ip-address;
        }
    }
}
proxy {
    source-address ip-address;
}
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
vlan vlan-id {
    immediate-leave;
    interface interface-name {
        group-limit limit;
        host-only-interface;
        immediate-leave;
        multicast-router-interface;
        static {
            group ip-address {
                source ip-address;
            }
        }
    }
}
proxy {
    source-address ip-address;
}
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
}
Syntax (QFX Series)

igmp-snooping {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
    flag flag (detail | disable | receive | send);
  }
  vlan (vlan-name | all) {
    immediate-leave;
    interface interface-name {
      group-limit limit;
      host-only-interface;
      immediate-leave;
      multicast-router-interface;
      static {
        group multicast-ip-address;
      }
    }
  }
  (l2-querier | igmp-querier (QFabric Systems only)) {
    source-address ip-address;
  }
  proxy {
    source-address ip-address;
  }
  query-interval seconds;
  query-last-member-interval seconds;
  query-response-interval seconds;
  robust-count number;
  version number;
}
Syntax (SRX Series)

```
igmp-snooping {
  vlan (all | vlan-name) {
    immediate-leave;
    interface interface-name {
      group-limit range;
      host-only-interface;
      multicast-router-interface;
      immediate-leave;
      static {
        group multicast-ip-address {
          source ip-address;
        }
      }
    }
  }
  l2-querier {
    source-address ip-address;
  }
  proxy {
    source-address ip-address;
  }
  qualified-vlan vlan-id;
  query-interval number;
  query-last-member-interval number;
  query-response-interval number;
  robust-count number;
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier>;
  }
}
```

Hierarchy Level

```
[edit bridge-domains bridge-domain-name protocols],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name protocols]
[edit routing-instances routing-instance-name protocols]
[edit protocols]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 18.1R1 for SRX1500 devices.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Description  Configure IGMP snooping to constrain multicast traffic to only the ports that have receivers attached. IGMP snooping enables the device to selectively send out multicast packets on only the ports that need them. Without IGMP snooping, the device floods the packets on every port. The device listens for the exchange of IGMP messages by the device and the end hosts. In this way, the device builds an IGMP snooping table that has a list of all the ports that have requested a particular multicast group. The factory default configuration enables IGMP snooping on all VLANs.

NOTE: IGMP snooping must be disabled on the device before enabling ISSU.

NOTE: Starting with Junos OS Release 18.1R1, QFX5110 switches support IGMP snooping in an EVPN-VXLAN multihoming environment, but in this environment you must enable IGMP snooping on all VLANs associated with any configured VXLANs. You cannot selectively enable IGMP snooping only on those VLANs that might have interested listeners, because all the VXLANs share VXLAN tunnel endpoints (VTEPs) between the same multihoming peers and must have the same settings.

Default  For most devices, IGMP snooping is disabled on the device by default, and you must configure IGMP snooping parameters in this statement hierarchy to enable it on one or more VLANs.

On legacy switches that do not support the Enhanced Layer 2 Software (ELS) configuration style, IGMP snooping is enabled by default on all VLANs, and the vlan statement includes a disable option if you want to disable IGMP snooping selectively on some VLANs or disable it on all VLANs.

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  • IGMP Snooping in MC-LAG Active-Active Mode

• Example: Configuring IGMP Snooping on SRX Series Devices

• IGMP Snooping Overview

• Example: Preserving Bandwidth with IGMP Snooping in an EVPN-VXLAN Environment
ignore

Syntax  ignore;

Hierarchy Level  [edit interfaces interface-name sonet-options trigger defect]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For ATM over SONET/SDH and SONET/SDH interfaces only, ignore a specific SONET/SDH defect trigger.

Default  If you do not include this statement, all defects are honored with no hold time.

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

Related Documentation  • Configuring SONET/SDH Defect Triggers
• hold-time (Physical Interface) on page 646

ignore-all

Syntax  ignore-all;

Hierarchy Level  [edit interfaces interface-name serial-options dce-options], [edit interfaces interface-name serial-options dte-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Ignore all control leads. You can include the ignore-all statement in the configuration only if you do not explicitly enable other signal handling options at the dte-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 Serial Signal Handling on page 324
**ignore-l3-incompletes**

**Syntax**  
`ignore-l3-incompletes;`

**Hierarchy Level**  
`[edit interfaces interface-name fastether-options],`  
`[edit interfaces interface-name gigether-options]`

**Release Information**  
Statement introduced in Junos OS Release 9.0.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

**Description**  
Ignore the counting of Layer 3 incomplete errors on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces.

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

**Related Documentation**  
- **• Ignoring Layer 3 Incomplete Errors**

**ilmi**

**Syntax**  
`ilmi;`

**Hierarchy Level**  
`[edit interfaces at-fpc/pic/port atm-options]`

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
Enable the router to communicate with directly attached ATM switches and routers. The router uses the VC 0.16 to communicate with the ATM switch or router. Once configured, you can display the IP address and port number of an ATM switch or router using the `show interfaces interface-name switch-id` command.

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

**Related Documentation**  
- **• Configuring Communication with Directly Attached ATM Switches and Routers**  
  - `show ilmi`  
  - `show ilmi statistics`
ima-group-options

Syntax
ima-group-options {
  differential-delay number;
  frame-length (32 | 64 | 128 | 256);
  frame-synchronization {
    alpha number;
    beta number;
    gamma number;
  }
  minimum-links number;
  symmetry (symmetrical-config-and-operation | symmetrical-config-asymmetrical-operation);
  test-procedure {
    ima-test-start;
    ima-test-stop;
    interface name;
    pattern number;
    period number;
  }
  transmit-clock (common | independent);
  version (1.0 | 1.1);
}

Hierarchy Level
[edit interfaces (t1-fpc/pic/port:m:n | e1-fpc/pic/port:n | t1|e1-fpc/pic/port)]

Release Information
Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description
Specify IMA group options.

Options
differential-delay msec—Maximum differential delay among links in msec.
  Range: 1 through 56
  Default: 25

frame-length (32 | 64 | 128 | 256)—IMA frame length in number of cells.
  Default: 128

frame-synchronization—IMA group frame synchronization selection.
  alpha number—Number of consecutive invalid ICP cells for IFSM.
    Range: 1 through 2
    Default: 2
  beta number—Number of consecutive errored ICP cells for IFSM.
    Range: 1 through 2
    Default: 2
gamma number—Number of consecutive valid ICP cells for IFSM.
Range: 1 through 5
Default: 1

minimum-links number—IMA group minimum active links.
Range: 1 through 8
Default: 1

symmetry (symmetrical-config-and-operation | symmetrical-config-asymmetrical-operation)—IMA group symmetry mode selection.

test-procedure—Specify an IMA link interface test.

  ima-test-start—Start IMA group test.
  ima-test-stop—Stop IMA group test.
  interface name—Interface name of the IMA link to test.

  pattern number—IMA test pattern.
  Range: 1 through 254
  Default: 170

  period seconds—Length of IMA pattern test in seconds.
  Range: 1 through 4,294,967,294.
  Default: 10

transmit-clock (common | independent)—Transmit clock configuration.
  Default: common

version (1.0 | 1.1)—IMA specification version.

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

Related Documentation
  • ATM Support on Circuit Emulation PICs Overview
  • ima-link-options on page 667
  • Understanding Inverse Multiplexing for ATM
ima-link-options

**Syntax**  ima-link-options group g

**Hierarchy Level**  [edit interfaces (t1-fpc/pic/port:m|n | t1|e1-fpc/pic/port)]

**Release Information**  Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**  Specify an interface as a member of an IMA group.

**Options**  group g—Implying at-x/y/g.

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

**Related Documentation**  • ATM Support on Circuit Emulation PICs Overview
• ima-group-options on page 665

inactivity-timeout

**Syntax**  inactivity-timeout seconds;

**Hierarchy Level**  [edit interfaces interface-name services-options]

**Release Information**  Statement introduced before Junos OS Release 7.4.

**Description**  For adaptive services interfaces, configure the inactivity timeout period for established flows. The timeout configured in the application protocol definition overrides this value.

**Options**  seconds—Timeout period, in seconds.
**Range:**  4 through 86,400 seconds
**Default:**  30 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 Services Interfaces Library for Routing Devices
incoming-map

Syntax
incoming-map { caller caller-number | accept-all; }

Hierarchy Level
[edit interfaces dln unit logical-unit-number dialer-options],
[edit logical-systems logical-system-name interfaces dln unit logical-unit-number dialer-options]

Release Information
Statement introduced in Junos OS Release 7.5.

Description
On J Series Services Routers with interfaces configured for ISDN, specify the dialer to accept incoming calls.

The remaining statements are explained separately. See CLI Explorer.

NOTE: The incoming-map statement is mandatory for the router to accept any incoming ISDN calls.

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

Related Documentation
• Junos OS Interfaces and Routing Configuration Guide
indication

Syntax indication (ignore | normal | require);

Hierarchy Level [edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For X.21 interfaces only, configure the from-DCE signal indication.

Options ignore—The from-DCE signal is ignored.
                normal—Normal indication signal handling as defined by ITU-T Recommendation X.21.
                require—The from-DCE signal must be asserted.
                Default: normal

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

Related Documentation • Configuring the Serial Signal Handling on page 324
indication-polarity

Syntax  
indication-polarity (negative | positive);

Hierarchy Level  
[edit interfaces interface-name serial-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For X.21 interfaces only, configure the indication signal polarity.

Options  
positive—Positive signal polarity.

negative—Negative signal polarity.

Default: positive

Required Privilege Level  
interface—To view this statement in the configuration.

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

Related Documentation  
• Configuring Serial Signal Polarities on page 327
**ingress-policer-overhead**

**Syntax**

```
ingress-policer-overhead bytes;
```

**Hierarchy Level**

```
[edit chassis fpc slot-number pic pic-number]
```

**Release Information**

Statement introduced before Junos OS Release 11.1.  
Statement introduced in Junos OS Release 15.1X49-D30 for vSRX.

**Description**

Add the configured number of bytes to the length of a packet entering the interface.

Configure a policer overhead to control the rate of traffic received on an interface. Use this feature to help prevent denial-of-service (DoS) attacks or to enforce traffic rates to conform to the service-level agreement (SLA). When you configure a policer overhead, the configured policer overhead value (bytes) is added to the length of the final Ethernet frame. This calculated length of frame is used to determine the policer or the rate-limiting action.

Traffic policing combines the configured policy bandwidth limits and the burst size to determine how to meter the incoming traffic. If you configure a policer overhead on an interface, Junos OS adds those bytes to the length of incoming Ethernet frames. This added overhead fills each frame closer to the burst size, allowing you to control the rate of traffic received on an interface.

You can configure the policer overhead to rate-limit queues and Layer 2 and Layer 3 policers, for standalone (SA) and high-availability (HA) deployments. The policer overhead and the shaping overhead can be configured simultaneously on an interface.

---

**NOTE:** vSRX supports policer overhead on Layer 3 policers only.

The policer overhead applies to all interfaces on the PIC. In the following example, Junos OS adds 10 bytes of overhead to all incoming Ethernet frames on ports ge-0/0/0 through ge-0/0/4.

```
set chassis fpc 0 pic 0 ingress-policer-overhead 10
```

---

**NOTE:** vSRX only supports fpc 0 pic 0. When you commit the ingress-policer-overhead statement, the vSRX takes the PIC offline and then back online.
You need to craft the policer overhead size to match your network traffic. A value that is too low will have minimal impact on traffic bursts. A value that is too high will rate-limit too much of your incoming traffic.

In this example, the policer overhead of 255 bytes is configured for ge-0/0/0 through ge-0/0/4. The firewall policer is configured to discard traffic when the burst size is over 1500 bytes. This policer is applied to ge-0/0/0 and ge 0/0/1. Junos OS adds 255 bytes to every Ethernet frame that comes into the configured ports. If, during a burst of traffic, the combined length of incoming frames and the overhead bytes exceeds 1500 bytes, the policer starts to discard further incoming traffic.

```
set chassis fpc 0 pic 0 ingress-policer-overhead 255
set interfaces ge-0/0/0 unit 0 family inet policer input overhead_policer
set interfaces ge-0/0/0 unit 0 family inet address 10.9.1.2/24
set interfaces ge-0/0/1 unit 0 family inet policer input overhead_policer
set interfaces ge-0/0/1 unit 0 family inet address 10.9.2.2/24
set firewall policer overhead_policer if-exceeding bandwidth-limit 32k
set firewall policer overhead_policer if-exceeding burst-size-limit 1500
set firewall policer overhead_policer then discard
```

**Options**

- **bytes**—Number of bytes added to a frame entering an interface.
- **Range**: 0–255 bytes
- **Default**: 0

```
[edit chassis fpc 0 pic 0]
user@host# set ingress-policer-overhead 10;
```

**Required Privilege Level**

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

**Related Documentation**

- *ingress-shaping-overhead*
- *Policer Overhead to Account for Rate Shaping Overview*
- *Example: Configuring Policer Overhead to Account for Rate Shaping*
- *Configuring a Policer Overhead*
- *CoS on Enhanced IQ2 PICs Overview*
**ingress-rate-limit**

**Syntax**

```
ingress-rate-limit rate;
```

**Hierarchy Level**

```
[edit interfaces interface-name fastether-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Perform port-based rate limiting on ingress traffic arriving on Fast Ethernet 8-port, 12-port, and 48-port PICs.

**Options**

- **rate**—Traffic rate, in megabits per second (Mbps).
- **Range**: 1 through 100 Mbps

**Required Privilege**

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

**Related Documentation**

- Configuring the Ingress Rate Limit
init-command-string

**Syntax**

`init-command-string initialization-command-string;`

**Hierarchy Level**

```
[edit interfaces umd0 modem-options]
```

**Release Information**

Statement introduced in Junos OS Release 8.2.

**Description**

For J Series Services Routers, configure the command string used to initialize the USB modem.

When you connect the USB modem to the USB port on a Services Router, the router applies the modem AT commands configured in the `init-command-string` command to the initialization commands on the modem.

For example, the initialization command string `ATS0=2\n` configures the USB modem to pick up a call after 2 rings.

If you do not include the `init-command-string` statement, the router applies the default initialization string to the modem.

**Options**

`initialization-command-string`—Specify an initialization command string using the following AT command values:

- `%C0`—Disables data compression.
- `&C1`—Disables reset of the modem when it loses the carrier signal.
- `&Q8`—Enables Microcom Networking Protocol (MNP) error control mode.
- `AT`—Attention. Informs the modem that a command follows.
- `E0`—Disables the display on the local terminal of commands issued to the modem from the local terminal.
- `Q0`—Enables the display of result codes.
- `S0=0`—Disables the auto-answer feature, whereby the modem automatically answers calls.
- `S7=45`—Instructs the modem to wait 45 seconds for a telecommunications service provider (carrier) signal before terminating the call.
- `V1`—Displays result codes as words.

**Default:** `AT S7=45 S0=0 V1 X4 &C1 E0 Q0 &Q8 %C0`

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
initial-route-check

Syntax

```
initial-route-check seconds;
```

Hierarchy Level

```
[edit interfaces dln unit logical-unit-number dialer-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

On J Series Services Routers with ISDN interfaces, allows the router to check whether the primary route is up after the initial startup of the router is complete and the timer expires.

Options

- `seconds`—How long to wait to check if the primary interface is up after the router comes up.
  - **Range:** 1 through 300 seconds
  - **Default:** 120 seconds

Required Privilege Level

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

Related Documentation

- ISDN Interfaces Overview
- Junos OS Interfaces and Routing Configuration Guide
inner-tag-protocol-id

Syntax

inner-tag-protocol-id tpid;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Release Information

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the IEEE 802.1Q TPID value to rewrite for the inner tag.

All TPIDs you include in input and output VLAN maps must be among those you specify at the [edit interfaces interface-name gigether-options ethernet-switch-profile tag-protocol-id [ tpid ] ] hierarchy level.

On MX Series routers, you can use this statement for Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs.

Default

If the inner-tag-protocol-id statement is not configured, the TPID value is 0x8100.

Required Privilege

Level

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

Related Documentation

• Configuring Inner and Outer TPIDs and VLAN IDs
inner-vlan-id

Syntax  inner-vlan-id number;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers or 100-Gigabit Ethernet Type 5 PIC with CFP, or on Ethernet interfaces on EX Series switches, specify the VLAN ID to rewrite for the inner tag of the final packet.

You cannot include the inner-vlan-id statement with the swap statement, swap-push statement, push-push statement, or push-swap statement and the inner-vlan-id statement at the [edit interfaces interface-name unit logical-unit-number output-vlan-map] hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the inner-vlan-id statement you include at the [edit interfaces interface-name unit logical-unit-number] hierarchy level.

Options  number—VLAN ID number.
Range: 0 through 4094

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

Related Documentation  • Configuring Inner and Outer TPIDs and VLAN IDs
inner-vlan-id-range

Syntax

inner-vlan-id-range start start-id end end-id;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],

Release Information

Statement introduced in Junos OS Release 9.0.

Description

The range of VLAN IDs to be used in the ATM-to-Ethernet interworking cross-connect. Specify the starting VLAN ID and ending VLAN ID.

Options

start-id—The lowest VLAN ID to be used.

end-id—The highest VLAN ID to be used.

Range: 32 through 4094

Required Privilege

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring ATM-to-Ethernet Interworking on page 262
input

Syntax

```plaintext
input { 
  service-set service-set-name <service-filter filter-name>; 
  post-service-filter filter-name; 
}
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet service],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more input service sets and filters, and one postservice filter to be applied to traffic.

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

• Junos OS Services Interfaces Library for Routing Devices
input-list

Syntax  
input-list [ filter-names ];

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

Release Information  
Statement introduced in Junos OS Release 7.6.

Description  
Apply a group of filters to evaluate when packets are received on an interface.

Options  
[ filter-names ]—Name of a filter to evaluate when packets are received on the interface.  
Up to 16 filters can be included in a filter input list.

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

Related Documentation  
• Applying a Filter to an Interface on page 220  
• Routing Policies, Firewall Filters, and Traffic Policers Feature Guide  
• Junos OS Administration Library  
• output-list on page 860
**input-policer**

**Syntax**

```
input-policer policer-name;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number layer2-policer]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number layer2-policer]
```

**Release Information**

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Apply a single-rate two-color policer to the Layer 2 input traffic at the logical interface. The `input-policer` and `input-three-color` statements are mutually exclusive.

**Options**

- `policer-name`—Name of the single-rate two-color policer that you define at the `[edit firewall]` hierarchy level.

**Usage Guidelines**

See Applying Layer 2 Policers to Gigabit Ethernet Interfaces.

**Required Privilege Level**

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

**Related Documentation**

- Two-Color and Three-Color Policers at Layer 2
- Applying Layer 2 Policers to Gigabit Ethernet Interfaces
- Configuring a Gigabit Ethernet Policer
- `input-three-color` on page 683
- `layer2-policer` on page 726
- `logical-interface-policer` on page 755
- `output-policer` on page 861
- `output-three-color` on page 863
input-priority-map

Syntax

```plaintext
input-priority-map {
    ieee802.1p premium [values ];
}
```

Hierarchy Level

[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]
[edit interfaces interface-name ether-options ethernet-switch-profile ethernet-policer-profile]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the input policer priority map to be applied to incoming frames on this interface.

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

- Specifying an Input Priority Map
- output-priority-map on page 862

```
input-three-color

Syntax  

```
input-three-color policer-name;
```

Hierarchy Level  

```
[edit interfaces interface-name unit logical-unit-number layer2-policer]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number layer2-policer]
```

Release Information  

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  

Apply a single-rate or two-rate three-color policer to the Layer 2 input traffic at the logical interface. The `input-three-color` and `input-policer` statements are mutually exclusive.

Options  

`policer-name`—Name of the single-rate or two-rate three-color policer.

Usage Guidelines  

See `Applying Layer 2 Policers to Gigabit Ethernet Interfaces`.

Required Privilege Level  

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

Related Documentation  

- Two-Color and Three-Color Policers at Layer 2
- Applying Layer 2 Policers to Gigabit Ethernet Interfaces
  - Configuring a Gigabit Ethernet Policer
- input-policer on page 681
- layer2-policer on page 726
- logical-interface-policer on page 755
- output-policer on page 861
- output-three-color on page 863
input-vlan-map (Aggregated Ethernet)

Syntax

```
input-vlan-map {
  (pop | push | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced in Junos OS Release 8.2.
Starting in Junos OS Release 17.3R1, input-vlan-map for outer vlan is supported for L2 circuit over aggregated Ethernet interfaces for QFX10000 Series switches.

Description

Define the rewrite profile to be applied to incoming frames on this logical interface. On MX Series routers, this statement only applies to aggregated Ethernet interfaces using Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ2 and IQ2-E interfaces and 100-Gigabit Ethernet Type 5 PIC with CFP.

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

- Stacking a VLAN Tag
- output-vlan-map (Aggregated Ethernet) on page 864
**input-vlan-map**

**Syntax**
```plaintext
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
```

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

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
- Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.
- Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

**Description**
For Gigabit Ethernet IQ, 10-Gigabit Ethernet SFPP interfaces, 100-Gigabit Ethernet Type 5 PIC with CFP only as well as Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces, define the rewrite profile to be applied to incoming frames on this logical interface.

The remaining statements are explained separately. See [CLI Explorer](#).

**NOTE:** Connectivity fault management (CFM) sessions for all interfaces in which `input-vlan-map` is configured are supported only if the interface also has an explicit configuration for `output-vlan-map` as `output-vlan-map pop;`. See [output-vlan-map](#). This configuration is required for all the interfaces in the topology even when the CFM session is on that interface or on a different interface in the data path of the same topology.

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

**Related Documentation**
- [Stacking a VLAN Tag](#)
- output-vlan-map on page 865
- Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
instance

Syntax  instance vpls-instance-name;

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management maintenance-domain name]


Description  Specify the VPLS instance of the default maintenance domain.

Required Privilege  Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring Maintenance Intermediate Points (MIPs)

• maintenance-domain on page 777

interface (Hierarchical CoS Schedulers)

Syntax  interface interface-name;

Hierarchy Level  [edit interfaces interface-set interface-set-name]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Specify an interface that is a member of the interface set. Supported on Ethernet interfaces on an MX Series router, Ethernet interfaces on IQ2E PIC on M Series and T Series routers, and IP demux interfaces on an MX Series router.

Required Privilege  Level  interface—To view this statement in the configuration.

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

Related Documentation  • Class of Service Feature Guide (Routers and EX9200 Switches)
interface (IEEE 802.1x)

**Syntax**
```plaintext
interface interface-id {
    maximum-requests integer;
    quiet-period seconds;
    reauthentication (disable | interval seconds);
    retries integer;
    server-timeout seconds;
    supplicant (single);
    supplicant-timeout seconds;
    transmit-period seconds;
}
```

**Hierarchy Level**
```plaintext
[edit protocols dot1x authenticator]
```

**Release Information**
Statement introduced in Junos OS Release 9.3.

**Description**
Use this statement to configure the 802.1x Port-Based Network Access Control protocol-specific Ethernet interface options.

**Default**
The default values are provided for the options below on the respective statement pages.

**Options**
- **maximum-requests**—Specify the maximum number of retransmission times for an EAPOL Request packet to the client before it times out the authentication session.
- **quiet-period**—Specify the number of seconds the port remains in the wait state following a failed authentication exchange with the client, before reattempting the authentication.
- **reauthentication**—Includes two options:
  - **disable**—Periodic reauthentication of the client is disabled.
  - **interval**—Specify the periodic reauthentication time interval.
- **retries**—Specify the number of tries after which the port remains in the wait state for quiet-period seconds before reattempting the authentication.
- **server-timeout**—Specify the number of seconds the port waits for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.
- **supplicant (single)**—Specify supplicant single mode. See the usage guidelines to configure other modes.
- **supplicant-timeout**—Specify the number of seconds the port waits for a response when relaying a request from the authentication server to the client before resending the request.
transmit-period—Specify the number of seconds the port waits before retransmitting the initial EAPOL PDUs 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**
- IEEE 802.1x Port-Based Network Access Control Overview
- authenticator on page 434
- dot1x on page 534
interface (IEEE 802.1ag OAM Connectivity-Fault Management)

Syntax

interface (interface-name | ((ge- | xe-) (fpc/pic/port | fpc/pic/port.unit-number | fpc/pic/port.unit-number vlan vlan-id)));

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]

Release Information

Statement introduced in Junos OS Release 8.4.

Description

For Ethernet interfaces on M320, MX Series, and T Series routers, configure IEEE 802.1ag Operation, Administration, and Management (OAM) support.

For Gigabit Ethernet interfaces and 10-Gigabit Ethernet interfaces on MX Series routers, configure IEEE 802.1ag Connectivity Fault Management (CFM) support on trunk interface ports.

Starting in Junos OS 17.4R1, you can enable support for IEEE 802.1ag CFM on pseudowire service interfaces by configuring maintenance intermediate points (MIPs) on the pseudowire service interfaces.

NOTE: The CFM MIP session is supported only on the pseudowire services interface and not on the pseudowire services tunnel interface.

Options

interface-name—Interface to which the MEP is attached. It could be a physical Ethernet interface, logical Ethernet interface, pseudowire services interfaces, or on a specific VLAN of a trunk port interface (MX Series only).

Required Privilege Level

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

Related Documentation

• Configuring a MEP to Generate and Respond to CFM Protocol Messages
interface (OAM Link-Fault Management)

Syntax

```plaintext
interface interface-name {
    apply-action-profile profile-name;
    link-discovery (active | passive);
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
    negotiation-options {
        allow-remote-loopback;
        no-allow-link-events;
    }
}
```

Hierarchy Level

```plaintext
[edit protocols oam ethernet link-fault-management]
```

Release Information

Statement introduced in Junos OS Release 8.2.

Description

For Ethernet interfaces on M320, MX Series, and T Series routers, configure IEEE 802.3ah Operation, Administration, and Management (OAM) support.

Options

- `interface interface-name`—Interface to be enabled for IEEE 802.3ah link fault management OAM support.

  The remaining statements are described separately.

Required Privilege Level

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

Related Documentation

- Enabling IEEE 802.3ah OAM Support
interface (Port Mirroring)

Syntax

interface interface-name {
    next-hop address;
}

Hierarchy Level
[edit forwarding-options port-mirroring family (inet | inet6) output]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the output interface for sending copies of packets elsewhere to be analyzed.

Options

interface-name—Name of the interface.

The remaining statements are explained separately. See CLI Explorer.

Usage Guidelines
See Configuring Port Mirroring on M, T MX, and PTX Series Routers.

Required Privilege

Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

interface-down

Syntax

interface-down;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name default-actions]

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Bring the interface down when a remote MEP connectivity failure is detected.

Required Privilege

Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
• Configuring a CFM Action Profile to Specify CFM Actions for CFM Events
**interface-name**

**Syntax**  
interface-name;

**Hierarchy Level**  
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],  
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include],

**Release Information**  
Statement introduced in Junos OS Release 10.0.

**Description**  
Append the interface name and VLAN ID or stacked VLAN ID to the username string used for authentication. The appended information takes the following format:

- For single VLAN—<interface-name>:<4-digit-vlan-id>
- For stack VLANs—<interface-name>:<4-digit-svlan-id>-<4-digit-vlan-id>

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

**Related Documentation**  
- Configuring VLAN Interface Username Information for AAA Authentication

**interface-none**

**Syntax**  
interface-none;

**Hierarchy Level**  
[edit protocols protection-group ethernet-ring ring-name east-interface]  
[edit protocols protection-group ethernet-ring ring-name west-interface]

**Description**  
Designates port as not used for Ethernet ring protection.

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

**Related Documentation**  
- Ethernet Ring Protection Switching Overview
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
# interface-range

**Syntax**

```plaintext
interface-range name {
  member-range interface-name-fpc/pic/port to interface-name-fpc/pic/port;
  member interface-name-fpc/pic/port;
  member interface-name-fpc/[low-high]/[*;
  member interface-name-fpc/[pic1,pic2,pic3...picN]/port
/*Common config is added as part of interface-range definition, as follows*/
  mtu 256;
  hold-time up 10;
  ether-options {
    flow-control;
    speed {
      100m;
    }
    802.3ad primary;
  }
}
```

**Hierarchy Level**

```
[edit interfaces]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.

**Description**

Specify a set of identical interfaces as an interface group, to which you can apply a common configuration to the entire set of interfaces. This group can consist of both lexical member ranges of interfaces specified using the `member-range interface-type-fpc/pic/port to xx-fpc/pic/port` option (regex not supported), and of individual or non-sequential members using the `member interface-type-fpc/pic/port` option (with regex support to specify the `fpc/pic/port` values).

**Options**

- **member-range**—Adds interfaces in lexical order. Regex is not supported.

  **Format:** `--member-range <start-range> to <end-range>`

  **Example:**
  ```
  --member-range ge-0/0/0 to ge-4/0/40;
  ```

- **member**—To add individual interfaces or multiple interfaces using regex.

  **Format:** `--member <list of interface names>`

  **Example:**
  ```
  --member ge-0/0/0;
  ```

  ```
  member ge-0/1/1;
  member ge-0/*/*;
  member ge-0/[1-10]/0;
  member ge-1/[1,3,6,10]/12
  ```
**interface-transmit-statistics**

**Syntax**

```
interface-transmit-statistics;
```

**Hierarchy Level**

```
[edit interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 11.4R3 for MX Series devices.

**Description**

Configure the interface to report the transmitted load statistics. If this statement is not included in the configuration, the interface statistics show the offered load on the interface, and not the actual transmitted load.

**Required Privilege Level**

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

**Related Documentation**

- Improvements to Interface Transmit Statistics Reporting on page 1160
- show interfaces on page 1161
interface-set (Ethernet Interfaces)

**Syntax**

```plaintext
interface-set interface-set-name {
    interface ethernet-interface-name {
        (unit unit-number | vlan-tags-outer vlan-tag);
    }
}
```

**Hierarchy Level**

[edit interfaces]

**Release Information**

Statement introduced in Junos OS Release 8.5.

**Description**

The set of interfaces used to configure hierarchical CoS schedulers on Ethernet interfaces on the MX Series router and IQ2E PIC on M Series and T Series routers.

The remaining statements are described separately.

**Required Privilege**

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

**Related Documentation**

- interface-set (Hierarchical Schedulers)
interface-set (IP Demux Interfaces)

Syntax

interface-set interface-set-name {
    interface interface-name {
        unit unit-number;
    }
}

Hierarchy Level
[edit interfaces]

Release Information
Statement introduced in Junos OS Release 9.2.

Description
The set of interfaces used to configure hierarchical CoS schedulers for subscribers on IP demux interfaces on the MX Series router.

The remaining statements are described separately.

Required Privilege

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

Related Documentation
• Junos Subscriber Access Configuration Guide
• Interfaces Fundamentals for Routing Devices
### interface-shared-with

**Syntax**  
interface-shared-with psdn;

**Hierarchy Level**  
[edit interfaces ge-fpc/pic/slot unit logical-unit-number],  
[edit interfaces so-fpc/pic/slot unit logical-unit-number],  
[edit interfaces xe-fpc/pic/slot unit logical-unit-number]

**Release Information**  
Statement introduced in Junos OS Release 9.3.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**  
Assign a logical interface under a shared physical interface to a Protected System Domain (PSD).

**Options**  
- $n$—PSD identification as a numeric value.  
  **Range:** 1 through 31

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

**Related Documentation**
**interface-status-tlv**

**Syntax**

```
interface-status-tlv [ down lower-layer-down ];
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name event]
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
```

**Release Information**


**Description**

Defines an action-profile consisting of various events and the action. Based on values of interface-status-tlv in the received CCM packets, specific action such as interface-down can be taken using action-profile options.

**Options**

- **down**—When the incoming CCM packet contains interface status TLV with value down, the action will be triggered for this action-profile.

- **lower-layer-down**—When the incoming CCM packet contains interface status TLV with value lower-layer-down, the action will be triggered for this action-profile.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Remote MEP Action Profile Support
interface-switch

Syntax
interface-switch connection-name {
    interface interface-name.unit-number;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols connections],
[edit protocols connections]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure Layer 2 switching cross-connects. The cross-connect is bidirectional, so packets received on the first interface are transmitted out the second interface, and those received on the second interface are transmitted out the first.

For Layer 2 switching cross-connects to work, you must also configure MPLS.

Options
connection-name—Connection name (up to 128 characters in Junos 12.3 and later).
interface interface-name.unit-number—Interface name. Include the logical portion of the name, which corresponds to the logical unit number.

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

Related Documentation
• Configuring the CCC Connection for Layer 2 Switching Cross-Connects
• Defining the Connection for Switching Cross-Connects on page 261
• MPLS Applications Feature Guide
interface-type (Interfaces)

Syntax
interface-type (bc | coc1 | ct1 | ct3 | dc | ds | so | t1 | t3);

Hierarchy Level
[edit interfaces interface-range name no-partition],
[edit interfaces interface-range name partition partition-number],
[edit interfaces interface-range name partition partition-number oc-slice oc-slice-range],
[edit interfaces interface-range name partition partition-number timeslot timeslot-range]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For IQ and IQE interfaces only, configure the sublevel interface type.

Options
bc—Dual—Port Channelized E1 and T1 ISDN PRI interface type. You can specify this
interface type at the [edit interfaces interface-name partition partition-number timeslot
timeslot-range] hierarchy level to create a bearer (B) channel bc-pim/0/port:channel
interface for each time you want to function as an ISDN PRI B-channel.

coc1—Channelized OC1 interface type. You can specify this interface type at the [edit
interfaces interface-name partition partition-number oc-slice oc-slice-range
interface-type coc12-fpc/pic/port] hierarchy level.

coc1—Channelized T1 interface type. You can specify this interface type at the [edit
interfaces interface-name partition partition-number interface-type
tct1-fpc/pic/port<:channel>] hierarchy level.

coc1—Channelized T3 interface type. You can specify this interface type at the [edit
interfaces interface-name partition partition-number oc-slice oc-slice-range
interface-type coc1-fpc/pic/port:channel no-partition] hierarchy level.

dc—Dual-Port Channelized E1 and T1 ISDN PRI interface type. You can specify this interface
type at the [edit interfaces interface-name partition partition-number timeslot
timeslot-range] hierarchy level to create a (D) channel dc-pim/0/port to control the
B-channels.

ds—DS0 interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number interface-type (ce1-fpc/pic/port |
tct1-fpc/pic/port<:channel>)] hierarchy level.

so—SONET/SDH interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number oc-slice oc-slice-range interface-type
coc12-fpc/pic/port] hierarchy level.

t1—T1 interface type. You can specify this interface type at the [edit interfaces
interface-name partition partition-number oc-slice oc-slice-range interface-type
(coc12-fpc/pic/port | coc1-fpc/pic/port)] hierarchy level.
t3—T3 interface type. You can specify this interface type at the `[edit interfaces
interface-name partition partition-number oc-slice oc-slice-range interface-type
(coc12-fpc/pic/port [ coc1-fpc/pic/port:channel no-partition])]` hierarchy level.

**Required Privilege**

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

**Related Documentation**

- Channelized E1 IQ and IQE Interfaces Overview
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
- Configuring Channelized T3 IQ Interfaces
## interfaces

| List of Syntax | Syntax (QFX Series) on page 702  
Syntax (EX Series, MX Series and T Series) on page 702 |
|---------------|--------------------------------------------------|
| Syntax (QFX Series) | interfaces interface-name {  
| | no-mac-learning;  
| | } |
| Syntax (EX Series, MX Series and T Series) | interfaces [ ... ] |
| QFX Series | [edit ethernet-switching-options] |
| EX Series, MX Series and T Series | [edit] |

### Release Information
Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for the QFX Series.

### Description
Configure settings for interfaces that have been assigned to family ethernet-switching.

### Default
The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

### Options
- **interface-name** — Name of an interface that is configured for family ethernet-switching.

  The remaining statement is 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.
- interface — To view this statement in the configuration.
- interface-control — To add this statement to the configuration.

### Related Documentation
- Physical Interface Configuration Statements Overview on page 48
- Configuring Aggregated Ethernet Link Protection
interfaces (Static and Dynamic Subscribers)

Syntax

```
interfaces {
  interface-name {
    unit logical-unit-number {
      actual-transit-statistics;
      auto-configure {
        agent-circuit-identifier {
          dynamic-profile profile-name;
        }
        line-identity {
          include {
            accept-no-ids;
            circuit-id;
            remote-id;
          }
          dynamic-profile profile-name;
        }
      }
      family family {
        access-concentrator name;
        address address;
        direct-connect;
        duplicate-protection;
        dynamic-profile profile-name;
      filter {
        adf {
          counter;
          input-precedence precedence;
          not-mandatory;
          output-precedence precedence;
          rule rule-value;
        }
        input filter-name {
          precedence precedence;
          shared-name filter-shared-name;
        }
        output filter-name {
          precedence precedence;
          shared-name filter-shared-name;
        }
      }
      max-sessions number;
      max-sessions-vsa-ignore;
      rpf-check {
        mode loose;
      }
      service {
        input {
          service-set service-set-name {
            service-filter filter-name;
          }
          post-service-filter filter-name;
        }
        output {
          service-set service-set-name {
            service-filter filter-name;
          }
          post-service-filter filter-name;
        }
      }
    }
  }
}
```
} } 
output { 
  service-set service-set-name { 
    service-filter filter-name; 
  } 
} } 

service-name-table table-name 
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max maximum-seconds>; 
unnumbered-address interface-name <preferred-source-address address>; 
} 
filter { 
  input filter-name { 
    precedence precedence; 
    shared-name filter-shared-name; 
  } 
  output filter-name { 
    precedence precedence; 
    shared-name filter-shared-name; 
  } 
} 
host-prefix-only; 
ppp-options { 
  chap; 
  pap; 
} 
proxy-arp; 

service { 
  pcef pcef-profile-name { 
    activate rule-name | activate-all; 
  } 
} 
targeted-options { 
  backup backup; 
  group group; 
  primary primary; 
  weight (junos-interface-target-weight | weight-value); 
} 

vlan-id; 

vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id]; 
} 

vlan-tagging; 
}
interface-set interface-set-name {
    interface interface-name {
        unit logical unit number {
            advisory-options {
                downstream-rate rate;
                upstream-rate rate;
            }
        }
    }
    pppoe-underlying-options {
        max-sessions number;
    }
}

demux0 {
  unit logical-unit-number {
    demux-options {
      underlying-interface interface-name
    }
    family family {
      access-concentrator name;
      address address;
      direct-connect;
      duplicate-protection;
      dynamic-profile profile-name;
      demux-source {
        source-prefix;
      }
      filter {
        input filter-name {
          precedence precedence;
          shared-name filter-shared-name;
        }
        output filter-name {
          precedence precedence;
          shared-name filter-shared-name;
        }
      }
      mac-validate (loose | strict):
      max-sessions number;
      max-sessions-vsa-ignore;
      rpf-check {
        fail-filter filter-name;
        mode loose;
      }
      service-name-table table-name
      short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max maximum-seconds>;
      unnumbered-address interface-name <preferred-source-address address>;
    }
    filter {
      input filter-name;
      output filter-name;
    }
    vlan-id number;
    vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
  }
}
pp0 {
  unit logical-unit-number {
    keepalive interval seconds;
    no-keepalives;
    pppoe-options {
      underlying-interface interface-name;
      server;
    }
  }
  ppp-options {
    aaa-options aaa-options-name;
    authentication [ authentication-protocols ];
    chap {
      challenge-length minimum minimum-length maximum maximum-length;
      local-name name;
    }
    ignore-magic-number-mismatch;
    initiate-ncp (dual-stack-passive | ipv6 | ip)
    ipcp-suggest-dns-option;
    mru size;
    mtu (size | use-lower-layer);
    on-demand-ip-address;
    pap;
    peer-ip-address-optional;
    local-authentication {
      password password;
      username-include {
        circuit-id;
        delimiter character;
        domain-name name;
        mac-address;
        remote-id;
      }
    }
  }
}
family inet {
  unnumbered-address interface-name;
  address address;
  service {
    input {
      service-set service-set-name {
        service-filter filter-name;
      }
      post-service-filter filter-name;
    }
    output {
      service-set service-set-name {
        service-filter filter-name;
      }
    }
  }
}
filter {
  input filter-name {
    precedence precedence;
    shared-name filter-shared-name;
  }
}
output filter-name {
    precedence precedence;
    shared-name filter-shared-name;
    }
}
}
}
}

Hierarchy Level  [edit dynamic-profiles profile-name]


Description  Define interfaces for dynamic client profiles.

Options  interface-name—The interface variable ($junos-interface-ifd-name). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.

NOTE: Though we do not recommend it, you can also enter the specific name of the interface you want to assign to 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  routing—To view this statement in the configuration.

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

Related Documentation  • Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles
  • Configuring Dynamic PPPoE Subscriber Interfaces
  • Configuring Dynamic VLANs Based on Agent Circuit Identifier Information
  • DHCP Subscriber Interface Overview
  • Subscribers over Static Interfaces Configuration Overview
  • Demultiplexing Interface Overview on page 293
interleave-fragments

Syntax
interleave-fragments;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For link services interfaces only, interleave long packets with high-priority packets.

Allows small delay-sensitive packets, such as Voice over IP (VoIP) packets, to interleave with long fragmented packets. This minimizes the latency of delay-sensitive packets.

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

Related Documentation
• Junos OS Services Interfaces Library for Routing Devices
### interval

**Syntax**

`interval (100ms | 10m | 10ms | 10s | 1m | 1s);`

**Hierarchy Level**

[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]

**Release Information**

Statement introduced in Junos OS Release 8.4.
Option `10ms` introduced in Junos OS Release 9.1.
Third-party interoperability during a unified in-service software upgrade (ISSU) introduced in Junos OS Release 17.1.

**Description**

Configure the interval between successive transmissions of continuity check messages (CCMs) as part of the connectivity fault detection strategy. When the receiving maintenance association end point (MEP) does not receive a CCM at the configured interval, the `loss-threshold` statement determines how many CCMs can be lost before the sending MEP is marked as down. The `hold-interval` statement then determines the frequency at which the database of MEPs in the maintenance association (MA) is flushed in the absence of updates.

During a unified in-service software upgrade (ISSU), Junos OS connectivity fault management (CFM) works when the peer device is not a Juniper Networks router. Interoperating with the router of another vendor, the Juniper Networks router retains session information and continues to transmit CCM (continuity check message) PDUs during the unified ISSU upgrade. For this feature to work, you must enable Packet Forwarding Engine keepalives with the `hardware-assisted-keepalives` statement, and configure the interval between CCMs to be 1 second with `interval` statement.

---

**NOTE:** For the continuity check message interval to be configured for 10 milliseconds, periodic packet management (PPM) runs on the Routing Engine and Packet Forwarding Engine by default. You can disable PPM only on the Packet Forwarding Engine. To disable PPM on the Packet Forwarding Engine, use the `no-delegate-processing` statement at the `[edit routing-options ppm]` hierarchy level.

---

**NOTE:** A continuity check interval of 10 milliseconds is not supported for CFM sessions over a label-switched interface (LSI).

**Options**

- **100ms**—100 milliseconds.
- **10m**—10 minutes.
10ms—10 milliseconds.
10s—10 seconds.
1m—1 minute.
1s—1 second.
Default: 1m

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

**Related Documentation**
- Continuity Check Protocol Parameters Overview
- Configuring Continuity Check Protocol Parameters for Fault Detection
- Configuring Connectivity Fault Management for Interoperability During Unified In-Service Software Upgrades

**inverse-arp**

**Syntax**
inverse-arp;

**Hierarchy Level**
- [edit interfaces interface-name unit logical-unit-number]
- [edit interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address multipoint-destination destination]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
For ATM encapsulation, enable responses to receive inverse ATM ARP requests. For Frame Relay encapsulation, enable responses to receive inverse Frame Relay ARP requests.

**Default**
Inverse ARP is disabled on all ATM and Frame Relay interfaces.

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

**Related Documentation**
- Configuring Inverse ATM1 or ATM2 ARP
- Configuring Inverse Frame Relay ARP
invert-data

Syntax
invert-data;

Hierarchy Level
[edit interfaces e1-fpc/pic/port],
[edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name e3-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description
Invert the transmission of unused data bits on the DS0, E1, E3, and T1 interface.

NOTE: When configuring E1 or T1 interfaces on 10-port Channelized E1/T1 IQE PICs, the invert-data statement must be included at the [edit interfaces e1-fpc/pic/port] or [edit interfaces t1-fpc/pic/port] hierarchy level as appropriate.

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

Related Documentation
• Configuring E1 Data Inversion
• Configuring E3 Data Inversion
• Configuring T1 Data Inversion
### ipsec-sa

**Syntax**  
```plaintext
ipsec-sa sa-name;
```

**Hierarchy Level**  
- `[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]`,  
- `[edit logical-systems logical-system-name interfaces es-fpc/pic/port unit logical-unit-number family inet]`

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
Specify the IP Security (IPsec) security association (SA) name associated with the interface.

**Options**  
- `sa-name`—IPsec security association name.

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

**Related Documentation**  
- [Junos OS Services Interfaces Library for Routing Devices](#)  
- [Junos OS Administration Library](#)
### isdn-options

**Syntax**

```plaintext
isdn-options {
    bchannel-allocation (ascending | descending);
    calling-number number;
    incoming-called-number number <reject>;
    spid1 spid-string;
    spid2 spid-string;
    static-tei-val value;
    switch-type (att5e | etsi | nil | ntdms100 | ntt);
    t310 seconds;
    tei-option (first-call | power-up);
}
```

**Hierarchy Level**

- [edit interfaces br-pim/0/port]
- [edit interfaces ct1-pim/0/port]
- [edit interfaces cel-pim/0/port]

**Release Information**

Statement introduced before Junos OS Release 7.4. 
`bchannel-allocation` option added in Junos OS Release 8.3.

**Description**

For J Series Services Routers only. Specify the ISDN options for configuring ISDN interfaces for group and user sessions.

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 ISDN Physical Interface Properties
- Allocating B-Channels for Dialout
- Junos OS Interfaces and Routing Configuration Guide
iteration-count

Syntax
iteration-count count-value;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id
  sla-iterator-profile profile-name]

Release Information
Statement introduced in Junos OS Release 11.1.

Description
Configure the number of iterations for which the connection partakes in the iterator for acquiring SLA measurements.

Options
count-value—Number of iterations for which the connection should partake in the iterator for acquiring SLA measurements.

Range: 1 through 65,535
Default: 0 (or infinite iterations)

Required Privilege
Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation
• sla-iterator-profile on page 998
• Configuring a Remote MEP with an Iterator Profile
iteration-period

Syntax  iteration-period iteration-period-value;

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]

Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description  Configure the iteration period, which is the maximum number of cycles per iteration (that is, the number of connections registered to an iterator cannot exceed this value).

Options  iteration-period-value—Maximum number of cycles per iteration.
Range: 1 through 2000
Default: 2000

Required Privilege  Level  Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation  • Configuring an Iterator Profile
• Configuring an Iterator Profile on a Switch (CLI Procedure)
keep-address-and-control

Syntax  keep-address-and-control;

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

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For interfaces with encapsulation type PPP CCC, do not remove the address and control bytes before encapsulating the packet into a tunnel.

Default  If you do not include this statement, address and control bytes are removed before encapsulating the packet into a tunnel.

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

Related Documentation  • Disabling the Removal of Address and Control Bytes on page 210
**keepalives**

**Syntax**

```
keepalives <interval seconds> <down-count number> <up-count number>;
```

**Hierarchy Level**

- `[edit interfaces interface-name]`
- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Enable the sending of keepalives on a physical interface configured with PPP, Frame Relay, or Cisco HDLC encapsulation.

For ATM2 IQ interfaces only, you can enable keepalives on a logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- `atm-ppp-llc`—PPP over AAL5 LLC encapsulation.
- `atm-ppp-vc-mux`—PPP over AAL5 multiplex encapsulation.

**Default**

Sending of keepalives is enabled by default. The default keepalive interval is 10 seconds for PPP, Frame Relay, or Cisco HDLC. The default down-count is 3 and the default up-count is 1 for PPP or Cisco HDLC.

**Options**

- **down-count number**—The number of keepalive packets a destination must fail to receive before the network takes down a link.
  
  **Range**: 1 through 255
  
  **Default**: 3

- **interval seconds**—The time in seconds between successive keepalive requests.
  
  **Range**: 1 through 32767 seconds
  
  **Default**: 10 seconds

- **up-count number**—The number of keepalive packets a destination must receive to change a link's status from down to up.
  
  **Range**: 1 through 255
  
  **Default**: 1

**Required Privilege Level**

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

**Related Documentation**

- Configuring Keepalives on page 118
- Configuring Frame Relay Keepalives
Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface

**key**

**Syntax**
```
key number;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number tunnel],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For Adaptive Services PICs on M Series routers (except the M320 and M120 routers), identify an individual traffic flow within a tunnel, as defined in RFC 2890, *Key and Sequence Number Extensions to GRE*.

**Options**
```
number—Value of the key.
Range: 0 through 4,294,967,295
```

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

**Related Documentation**
- *Junos OS Services Interfaces Library for Routing Devices*
l2tp-interface-id

Syntax
l2tp-interface-id name;
( dedicated | shared);

Hierarchy Level
[edit interfaces sp-fpc/pic/port unit logical-unit-number interface],
[edit logical-systems logical-system-name interfaces sp-fpc/pic/port unit logical-unit-number interface]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the L2TP options for configuring logical interfaces for group and user sessions.

Options
( dedicated | shared)—Specifies whether a logical interface can host one (dedicated) or multiple (shared) sessions at one time.

name—Interface identifier that must be replicated at the [edit access profile name] hierarchy level.

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

Related Documentation
• Junos OS Services Interfaces Library for Routing Devices
lACP (Protocols)

Syntax

```
lacp {
  traceoptions {
    file <filename> <files number> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  fast-hello-issu;
  ppm (Ethernet Switching) centralized;
}
```

Hierarchy Level

[edit protocols]

Release Information

Statement introduced in Junos OS Release 9.3.
The `ppm centralized` option introduced in Junos OS Release 9.4.
The `fast-hello-issu` option introduced in Junos OS Release 14.1.

Description

On MX and T Series routers, you can specify periodic packet management (PPM) as centralized. By default, the PPM is distributed.

MX Series routers support Link Aggregation Control Protocol (LACP) with fast hellos during unified ISSU. This support is disabled by default. You must enable the `fast-hello-issu` option on the main router and on the peer routers before starting unified ISSU. Note that the peer router must also be an MX Series router for this functionality to work.

Default

Distributed PPM processing is enabled for all packets that use PPM.

Options

- `ppm`—Set PPM to centralized.
- `fast-hello-issu`—Enable LACP with fast hellos during unified ISSU.

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

- Tracing LACP Operations
- Unified ISSU System Requirements
**lACP (802.3AD)**

**Syntax**
```
lACP {
  port-priority port-priority,
}
```

**Hierarchy Level**
[edit interfaces interface-name fastether-options 802.3ad],
[edit interfaces interface-name gigether-options 802.3ad]

**Release Information**
Statement introduced in Junos OS Release 9.3.

**Description**
Configure the Link Aggregation Control Protocol (LACP) port priority for Ethernet interfaces.

**Options**
- `port-priority`—Priority for being elected as the active port to collect and distribute traffic.
  - A smaller value indicates a higher priority for selection.
  - **Range:** 0 through 65,535
  - **Default:** 127

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

**Related Documentation**
- [Configuring LACP for Aggregated Ethernet Interfaces](#)
- [port-priority on page 907](#)
lACP (Aggregated Ethernet)

List of Syntax  
Syntax (NFX Series) on page 723  
Syntax (EX Series) on page 723

Syntax (NFX Series)  
lACP (active | passive) {  
  admin-key key;  
  fast-failover;  
  link-protection {  
    disable;  
    (revertive | non-revertive);  
  }  
  periodic interval  
  system-ID mac-address;  
  system-priority priority;  
  force-up;  
}

Syntax (EX Series)  
lACP {  
  (active | passive);  
  admin-key key;  
  accept-data;  
  fast-failover;  
  link-protection {  
    disable;  
    (revertive | non-revertive);  
  }  
  periodic interval;  
  system-id mac-address;  
  system-priority priority;  
}

Hierarchy Level (EX Series)  
[edit interfaces aeX aggregated-ether-options]  
[edit logical-systems logical-system-name interfaces aeX aggregated-ether-options]

Hierarchy Level (NFX Series)  
[edit interfaces interface-name aggregated-ether-options]

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.  
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  
Configure the Link Aggregation Control Protocol (LACP) parameters for interfaces. The remaining statement is explained separately.

For EX Series, when you configure the accept-data statement at the [edit interfaces aeX aggregated-ether-options lACP] hierarchy level, the router processes packets received on a member link irrespective of the LACP state if the aggregated Ethernet bundle is up.
NOTE: When you configure the accept-data statement at the [edit interfaces aeX aggregated-ether-options lacp] hierarchy level, this behavior occurs:

- By default, the accept-data statement is not configured when LACP is enabled.
- You can configure the accept-data statement to improve convergence and reduce the number of dropped packets when member links in the bundle are enabled or disabled.
- When LACP is down and a member link receives packets, the router or switch does not process packets as defined in the IEEE 802.1ax standard. According to this standard, the packets should be dropped, but they are processed instead because the accept-data statement is configured.

NOTE: The force-up statement is not supported on QFX10002 switches.

**Default**
If you do not specify LACP as either active or passive, LACP remains passive.

**Options**
- **active**—Initiate transmission of LACP packets.
- **admin-key number**—Specify an administrative key for the router or switch.

**fast-failover**—Specify to override the IEEE 802.3ad standard and allow the standby link to receive traffic. Overriding the default behavior facilitates subsecond failover.

- **passive**—Respond to LACP packets.

The remaining statements are explained separately. See CLI Explorer.

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

- Configuring Link Aggregation
- Configuring Aggregated Ethernet LACP (CLI Procedure)
- Understanding Aggregated Ethernet Interfaces and LACP for Switches
- Configuring LACP for Aggregated Ethernet Interfaces
layer2-policer

Syntax

layer2-policer {
  input-policer policer-name;
  input-three-color policer-name;
  output-policer policer-name;
  output-three-color policer-name;
}

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

For 1-Gigabit Ethernet and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces on M Series, MX Series, and T Series routers, and for aggregated Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces on EX Series switches, apply Layer 2 logical interface policers. The following policers are supported:

- Two-color
- Single-rate tricolor marking (srTCM)
- Two-rate tricolor marking (trTCM)

Two-color and tricolor policers are configured at the [edit firewall] hierarchy level.

Options

input-policer policer-name—Two-color input policer to associate with the interface. This statement is mutually exclusive with the input-three-color statement.

input-three-color policer-name—Tricolor input policer to associate with the interface. This statement is mutually exclusive with the input-policer statement.

output-policer policer-name—Two-color output policer to associate with the interface. This statement is mutually exclusive with the output-three-color statement.

output-three-color policer-name—Tricolor output policer to associate with the interface. This statement is mutually exclusive with the output-policer statement.

Required Privilege Level

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

Related Documentation

- Applying Layer 2 Policers to Gigabit Ethernet Interfaces
- Configuring Gigabit Ethernet Two-Color and Tricolor Policers
**lcp-max-conf-req**

**Syntax**  
```
lcp-max-conf-req number
```

**Hierarchy Level**  
```
[edit interfaces so-fpc/pic/port unit number ppp-options]
```

**Release Information**  

**Description**  
Set the maximum number of LCP Configure-Requests to be sent, after which the router goes to LCP down state.

**Options**  
`number`—From 0 to 65,535, where 0 means send infinite LCP Configure-Requests, and any other value specifies the maximum number LCP Configure-Requests to send and then stop sending.

**Default**  
254

**Required Privilege Level**  
interface—To view this statement in the configuration.

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

**Related Documentation**  
- Configuring the LCP Configure-Request Maximum Sent on page 178
- `ppp-options` on page 910
lcp-restart-timer

Syntax  lcp-restart-timer milliseconds;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number ppp-options],
  [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]


Description  For interfaces with PPP, PPP TCC, PPP over Ethernet, PPP over ATM, and PPP over Frame Relay encapsulations, configure a restart timer for the Link Control Protocol (LCP) component of a PPP session.

Options  milliseconds—The time, in milliseconds, between successive LCP configuration requests.
  Range:  20 through 10000 milliseconds
  Default:  3 seconds

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

Related Documentation  • Configuring the PPP Restart Timers on page 177
level

Syntax  level number;

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]


Description  A number used in connectivity fault management (CFM) messages to identify the maintenance association. The number is embedded in each of the CFM frames. CFM messages within a given level are processed by maintenance end points (MEPs) at the same level. For example, the operator domain can be level 0, the provider domain can be level 3, and the customer domain can be level 7.

Options  number—A number used to identify the maintenance domain to which the CFM message belongs. 
  Range: 0 through 7

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

Related Documentation
• Creating a Maintenance Domain
**line-encoding**

**Syntax**

```
line-encoding (ami | b8zs);
```

**Hierarchy Level**

```
[edit interfaces ct1-fpc/pic/port],
[edit interfaces interface-name t1-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**

Set the line encoding format on the T1 interface.

---

**NOTE:** When configuring CT1 interfaces on the 10-port Channelized E1/T1 IQE PIC, the line-encoding statement must be included at the [edit interfaces ct1-fpc/pic/port] hierarchy level.

**Default**

The default line encoding is B8ZS.

**Options**

- `ami`—Use Alternate Mark Inversion (AMI) line encoding.
- `b8zs`—Use bipolar with 8-zeros substitution (B8ZS) line encoding.

**Required Privilege Level**

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

**Related Documentation**

- *Configuring T1 Line Encoding*
line-protocol

Syntax

    line-protocol protocol;

Hierarchy Level

    [edit interfaces interface-name serial-options]

Release Information

    Statement introduced before Junos OS Release 7.4.

Description

    For serial interfaces only, configure the line protocol.

Options

    protocol—You can specify the one of the following line protocols:
    • eia530—Line protocol EIA-530
    • v.35—Line protocol V.35
    • x.21—Line protocol X.21

Required Privilege

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

Related Documentation

    • Configuring the Serial Line Protocol on page 318
**line-rate**

**Syntax**

```
line-rate line-rate;
```

**Hierarchy Level**

```editor
[edit interfaces interface-name shdsl-options],
[edit logical-systems logical-system-name interfaces interface-name shdsl-options]
```

**Release Information**

Statement introduced in Junos OS Release 7.4.

**Description**

For J Series Services Routers only, configure the SHDSL line rate.

**Options**

`line-rate`—SHDSL line rate, in Kbps. Possible values are:

- **2-wire** (Kbps): 192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, 2304, auto

- **4-wire** (Kbps): 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, 4608

**Default:** For 2-wire mode, **auto**; for 4-wire mode, **4608** Kbps

**Required Privilege**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.
### linear-red-profile

**Syntax**

 linear-red-profile *profile-name*;

**Hierarchy Level**

[edit interfaces at-fpc/pic/port atm-options scheduler-maps map-name forwarding-class class-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, assign a linear RED profile to a specified forwarding class. To define the linear RED profiles, include the `linear-red-profiles` statement at the [edit interfaces at-fpc/pic/port atm-options] hierarchy level.

**Default**

If you do not include either the `epd-threshold` or the `linear-red-profile` statement in the forwarding class configuration, the Junos OS uses an EPD threshold based on the available bandwidth and other parameters.

**Options**

`profile-name`—Name of the linear RED profile.

**Required Privilege Level**

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

**Related Documentation**

- Configuring an ATM Scheduler Map
- linear-red-profiles on page 734
- Applying Scheduler Maps to ATM Interfaces
- `epd-threshold`
linear-red-profiles

Syntax

```
linear-red-profiles profile-name {
  high-plp-threshold percent;
  low-plp-threshold percent;
  queue-depth cells;
}
```

Hierarchy Level

```
[edit interfaces at-fpc/pic/port atm-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For ATM2 IQ interfaces only, define CoS virtual circuit drop profiles for RED. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.

Options

```
profile-name—Name of the drop 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

- ATM2 IQ VC Tunnel CoS Components Overview
- Configuring Linear RED Profiles on ATM Interfaces
link-adjacency-loss

Syntax        link-adjacency-loss;

Hierarchy Level [edit protocols oam ethernet link-fault-management action-profile event ]

Release Information Statement introduced in Junos OS Release 8.5.

Description Loss of adjacency with IEEE 802.3ah link-fault management peer event. When included, the loss-of-adjacency event triggers the action specified under the action statement.

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

Related Documentation • Monitoring the Loss of Link Adjacency

link-discovery

Syntax        link-discovery (active | passive);

Hierarchy Level [edit protocols oam ethernet link-fault-management interface interface-name ]

Release Information Statement introduced in Junos OS Release 8.2.

Description For Ethernet interfaces on EX Series switches, and M320, M120, MX Series, and T Series routers, specify the discovery mode used for IEEE 802.3ah Operation, Administration, and Management (OAM) support. The discovery process is triggered automatically when OAM 802.3ah functionality is enabled on a port. Link monitoring is done when the interface sends periodic OAM PDUs.

Options (active | passive)—Passive or active mode. In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. In passive mode, the peer initiates the discovery process. Once the discovery process is initiated, both sides participate in discovery.

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

Related Documentation • Configuring Link Discovery
link-down

Syntax     link-down;

Hierarchy Level   [edit protocols oam ethernet link-fault-management ]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Mark the interface down for transit traffic.

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

Related Documentation
-  *Specifying the Actions to Be Taken for Link-Fault Management Events*

link-event-rate

Syntax     link-event-rate {  
        frame-error count;  
        frame-period count;  
        frame-period-summary count;  
        symbol-period count;  
    }

Hierarchy Level   [edit protocols oam ethernet link-fault-management action-profile event ]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Configure the number of link-fault management events per second.

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

Related Documentation
-  *Configuring Threshold Values for Fault Events in an Action Profile*
link-fault-management

Syntax

```
link-fault-management {
  action-profile profile-name {
    action {
      link-down;
      send-critical-event;
      syslog;
    }
    event {
      link-adjacency-loss;
      link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
      }
      protocol-down;
    }
  }
  interface interface-name {
    apply-action-profile profile-name;
    link-discovery (active | passive);
    loopback-tracking;
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    negotiation-options {
      allow-remote-loopback;
      no-allow-link-events;
    }
  }
}
```

Hierarchy Level

[edit protocols oam ethernet]

Release Information

Statement introduced in Junos OS Release 8.2.

Description

For Ethernet interfaces on M320, M120, MX Series, and T Series routers and EX Series switches, specify fault signaling and detection for IEEE 802.3ah Operation, Administration, and Management (OAM) support.

The remaining statements are explained separately. See CLI Explorer.
link-layer-overhead

Syntax  
link-layer-overhead percent;

Hierarchy Level  
[edit interfaces interface-name m1fr-uni-nni-bundle-options],  
[edit interfaces interface-name unit logical-unit-number],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For AS PIC or MultiServices PIC link services IQ interfaces (lsq) only, configure the percentage of total bundle bandwidth to be set aside for link-layer overhead.

Options  
percent—Percentage of total bundle bandwidth to be set aside for link-layer overhead.  
Range: 0 through 50 percent  
Default: 4 percent

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

Related Documentation  
• Enabling IEEE 802.3ah OAM Support  
• Junos OS Services Interfaces Library for Routing Devices
link-mode

Syntax  
link-mode mode (automatic | full-duplex | half-duplex);

Hierarchy Level  
[edit interfaces interface-name],
[edit interfaces interface-name ether-options],
[edit interfaces ge-pim/0/0 switch-options switch-port port-number]

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 12.2 for ACX Series Universal Metro Routers.

Description  
Set the device’s link connection characteristic.

Options  
mode—Link characteristics:

• automatic—Link mode is negotiated. This is the default for EX Series switches.
• full-duplex—Connection is full duplex.
• half-duplex—Connection is half duplex.

Default: Fast Ethernet interfaces can operate in either full-duplex or half-duplex mode. The router’s or switch’s management Ethernet interface, fpx0 or em0, and the built-in Fast Ethernet interfaces on the FIC (M7i router) autonegotiate whether to operate in full-duplex or half-duplex mode. Unless otherwise noted here, all other interfaces operate only in full-duplex mode.

NOTE: On EX Series switches, if no-auto-negotiation is specified in [edit interfaces interface-name ether-options], you can select only full-duplex or half-duplex. If auto-negotiation is specified, you can select any mode.

NOTE:
• Member links of an aggregated Ethernet bundle must not be explicitly configured with a link mode. You must remove any such link-mode configuration before committing the aggregated Ethernet configuration.
• Starting with Junos OS release 17.4R1 and later, the link-mode configuration is not supported for 10-Gigabit Ethernet interfaces.
• Starting in Junos OS release 18.4R1, half-duplex mode is supported on SRX340 and SRX345 devices.
**Required Privilege Level**

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

**Related Documentation**

- [Configuring the Link Characteristics on Ethernet Interfaces](#)
- [Understanding Management Ethernet Interfaces on page 10](#)
- [Configuring Gigabit Ethernet Interfaces (CLI Procedure)](#)
- [Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support](#)
link-protection

Syntax

```plaintext
link-protection {
  disable;
  (revertive | non-revertive);
}
```

Hierarchy Level

- [edit interfaces aex aggregated-ether-options]
- [edit interfaces aex aggregated-ether-options lacp]

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 15.1F4 for PTX Series routers.
Support for disable, revertive, and non-revertive statements added in Junos OS Release 9.3.

Description

On the router, for aggregated Ethernet interfaces only, configure link protection. In addition to enabling link protection, a primary and a secondary (backup) link must be configured to specify what links egress traffic should traverse. To configure primary and secondary links on the router, include the primary and backup statements at the [edit interfaces ge-fpc/pic/port gigether-options 802.3ad aex] hierarchy level or the [edit interfaces fe-fpc/pic/port fastether-options 802.3ad aex] hierarchy level.

On the switch, you can configure either Junos OS link protection for aggregated Ethernet interfaces or the LACP standards link protection for aggregated Ethernet interfaces.

For Junos OS link protection, specify `link-protection` at the following hierarchy levels:

- [edit interfaces ge-fpc/pic/port ether-options 802.3ad aex]
- [edit interfaces xe-fpc/pic/port ether-options 802.3ad aex] hierarchy level or at the [edit interfaces xe-fpc/pic/port ether-options 802.3ad aex] hierarchy level.

To disable link protection, use the `delete interface ae aggregate-ether-options link-protection` statement at the [edit interfaces aex aggregated-ether-options] hierarchy level or the [edit interfaces aex aggregated-ether-options lacp]] hierarchy level.

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

- Configuring Aggregated Ethernet Link Protection
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces for Switches
**link-speed (Aggregated Ethernet)**

**Syntax**

```
link-speed speed;
```

**Hierarchy Level (EX Series)**

- [edit interfaces aex aggregated-ether-options],
- [edit interfaces interface-range name aggregated-ether-options],
- [edit interfaces interface-range name aggregated-sonet-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
mixed option added in Junos OS Release 15.1F3 and 16.1R2 for PTX5000 routers and 15.1F6 and 16.1R2 for PTX3000 routers.

**Description**

For aggregated Ethernet interfaces only, set the required link speed.

**Options**

*speed*—For aggregated Ethernet links, you can specify *speed* in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation *k* (1000), *m* (1,000,000), or *g* (1,000,000,000).

Aggregated Ethernet links on the M120 router can have one of the following speeds:

- **100m**—Links are 100 Mbps.
- **10g**—Links are 10 Gbps.
- **1g**—Links are 1 Gbps.
- **oc192**—Links are OC192 or STM64c.

Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speeds:

- **10m**—Links are 10 Mbps.
- **100m**—Links are 100 Mbps.
- **1g**—Links are 1 Gbps.
- **10g**—Links are 10 Gbps.

Aggregated Ethernet links on T Series, MX Series, PTX Series routers, and QFX5100, QFX10002, QFX10008, and QFX10016 switches can be configured to operate at one of the following speeds:

- **100g**—Links are 100 Gbps.
- **100m**—Links are 100 Mbps.
- **10g**—Links are 10 Gbps.
- **1g**—Links are 1 Gbps.
- **40g**—Links are 40 Gbps.
- **50g**—Links are 50 Gbps.
- **80g**—Links are 80 Gbps.
- **8g**—Links are 8 Gbps.
- **mixed**—Links are of various speeds.
- **oc192**—Links are OC192.

**mixed**—Enables bundling of different Ethernet rate links in the same Aggregated Ethernet interface.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**
- *Aggregated Ethernet Interfaces Overview*
- *Configuring Aggregated Ethernet Link Speed on page 102*
- *Configuring Mixed Rates and Mixed Modes on Aggregated Ethernet Bundles*
- *Configuring Aggregated Ethernet Links (CLI Procedure)*
- *Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch*
**link-speed (Aggregated SONET/SDH)**

**Syntax**
```
link-speed (speed | mixed);
```

**Hierarchy Level**
```
[edit interfaces asx aggregated-sonet-options]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.  
mixed option added in Release 8.0.

**Description**
For aggregated SONET/SDH interfaces only, set the required link speed.

**Options**

- `speed`—Aggregated SONET/SDH links can have one of the following speed values.
  - `oc3`—Links are OC3c or STM1c.
  - `oc12`—Links are OC12c or STM4c.
  - `oc48`—Links are OC48c or STM16c.
  - `oc192`—Links are OC192c or STM64c.
  - `oc768`—Links are OC768c or STM256c.

- `mixed`—For aggregated SONET/SDH links on T Series routers, you can mix interface speeds in SONET/SDH aggregation bundles. Interface speeds from OC3 through OC768 are supported.

**Required Privilege Level**

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

**Related Documentation**
- Configuring Aggregated Ethernet Link Speed on page 102
- Configuring Aggregated SONET/SDH Interfaces
linktrace

Syntax

`linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size `path-database-size`;
}

Hierarchy Level

`[edit protocols oam ethernet connectivity-fault-management]`

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Configure connectivity fault management linktrace parameters.

Required Privilege Level

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

Related Documentation

- Configuring Linktrace Protocol in CFM
lmi (Frame Relay)

Syntax

```plaintext
lmi {
    lmi-type (ansi | itu | c-lmi);
    n391dte number;
    n392dce seconds;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte number;
    t392dce seconds;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Set Frame Relay keepalive parameters.

Options

**n391dte**—DTE full status polling interval.
- **Range:** 1 through 255
- **Default:** 6

**n392dce**—DCE error threshold, in number of errors.
- **Range:** 1 through 10
- **Default:** 3

**n392dte**—DTE error threshold, in number of errors.
- **Range:** 1 through 10
- **Default:** 3

**n393dce**—DCE monitored event-count.
- **Range:** 1 through 10
- **Default:** 4

**n393dte**—DTE monitored event-count.
- **Range:** 1 through 10
- **Default:** 4

**t391dte**—DTE polling timer.
- **Range:** 5 through 30 seconds
- **Default:** 10 seconds

**t392dce**—DCE polling timer.
- **Range:** 5 through 30 seconds
- **Default:** 15 seconds
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 Tunable Keepalives for Frame Relay LMI on page 749
- lmi-type on page 749
- mlf-un-nni-bundle-options on page 790
lmi (Ethernet OAM)

Syntax

```
lmi {
    status-counter count;
    polling-verification-timer value;
    interface name {
        uni-id uni-name;
        status-counter number;
        polling-verification-timer value;
        evc-map-type (all-to-one-bundling | bundling | service-multiplexing);
        evc evc-name {
            default-evc;
            vlan-list vlan-id-list;
        }
    }
}
```

Hierarchy Level
[edit protocols oam ethernet]

Release Information
Statement introduced in Junos OS Release 9.5.

Description
On routers with ge, xe, or ae interfaces, configure an OAM Ethernet Local Management Interface (E-LMI).

NOTE: On MX Series routers, E-LMI is supported on Gigabit Ethernet (ge), 10-Gigabit Ethernet (xe), and Aggregated Ethernet (ae) interfaces configured on MX Series routers with DPC only.

Options

- **status-counter count**—Status counter (N393), defaults to 4.
- **interface name**—Polling verification timer (T392), defaults to 15 seconds.
- **uni-id uni-name**—(Optional) Defaults to the physical interface name.
- **status-counter number**—(Optional) Defaults to a global value.
- **polling-verification-timer value**—(Optional) Defaults to a global value.
- **evc-map-type (all-to-one-bundling | bundling | service-multiplexing)**—Specify the Ethernet virtual connection (EVC) map type.
- **evc evc-name**—Specify the name of the EVC.
- **default-evc**—Set the specified EVC as the default EVC.
- **vlan-list vlan-id-list**—Specify a group of VLANs to assign to the EVC.
### lmi-type

**Syntax**

```
lmi-type (ansi | itu | c-lmi);
```

**Hierarchy Level**

```
[edit interfaces interface-name lmi],
[edit interfaces interface-name mlfr-uni-nni-bundle-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Set Frame Relay Local Management Interface (LMI) type.

---

**NOTE:** Consortium LMI is supported on all MPCs and I-chip based FPCs.

**Options**

- **ansi**—Use ANSI T1.617 Annex D LMIs.
- **itu**—Use ITU Q933 Annex A LMIs.
- **c-lmi**—Use Consortium LMI.

**Default:** ansi

---

**Required Privilege Level**

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

**Related Documentation**

- Configuring Frame Relay Keepalives
- mlfr-uni-nni-bundle-options on page 790
- lmi (Frame Relay) on page 746
- Junos OS Services Interfaces Library for Routing Devices
load-interval

Syntax

load-interval seconds;

Hierarchy Level

[edit interfaces dl unit logical-unit-number dialer-options],
[edit logical-systems logical-system-name interfaces dl unit logical-unit-number dialer-options]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

On J Series Services Routers with ISDN logical interfaces, specify the interval used to calculate the average load on the network. By default, the average interface load is calculated every 60 seconds.

Options

seconds—Number of seconds at which the average load calculation is triggered.

Range: 20 through 180, in 10-second intervals

Default: 60 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 Interfaces and Routing Configuration Guide
**load-threshold**

**Syntax**

load-threshold *percent*;

**Hierarchy Level**

[edit interfaces dln *unit logical-unit-number* dialer-options],
[edit logical-systems *logical-system-name* interfaces dln *unit logical-unit-number* dialer-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

On J Series Services Routers with ISDN logical interfaces, specify the bandwidth threshold percentage used for adding interfaces. Another link is added to the multilink bundle when the load reaches the threshold value you set. Specify a percentage between 0 and 100.

**Options**

*percent*—Bandwidth threshold percentage used for adding interfaces. When set to 0, all available channels are dialed.

- **Range**: 0 through 100 seconds
- **Default**: 100 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 Interfaces and Routing Configuration Guide
local-name

**Syntax**
local-name name;

**Hierarchy Level**
- [edit interfaces interface-name ppp-options chap]
- [edit interfaces interface-name ppp-options pap]
- [edit interfaces interface-name unit logical-unit-number ppp-options chap]
- [edit interfaces interface-name unit logical-unit-number ppp-options pap]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options chap]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options pap]
- [edit dynamic-profiles profile-name interfaces pp0 unit "$junos-interface-unit" ppp-options]
- [edit dynamic-profiles profile-name interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options]

**Release Information**

**Description**
Specify the name of the interface used for CHAP or PAP authentication. Dynamic interfaces are supported only for CHAP authentication.

For ATM2 IQ interfaces only, you can configure a CHAP local name on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- **atm-ppp-llc**—PPP over AAL5 LLC encapsulation.
- **atm-ppp-vc-mux**—PPP over AAL5 multiplex encapsulation.

**Options**

- **name**—Name of the interface used as an identifier in CHAP challenge and response packets or PAP request and response packets.

**Default:** When you do not include the `local-name` statement in the configuration, the interface sends the router’s system hostname in CHAP challenge and response packets or PAP request and response packets.

**Range:** For CHAP authentication, a string of 1 through 32 characters. For PAP authentication, a string of 1 through 8 characters.

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

**Related Documentation**
- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
### local-password

**Syntax**

```bash
local-password password;
```

**Hierarchy Level**

-[edit interfaces interface-name ppp-options pap],
-[edit interfaces interface-name unit logical-unit-number ppp-options pap],
-[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options pap]

**Release Information**

Statement introduced in Junos OS Release 8.3.

**Description**

Configure the host password for sending PAP requests.

**Required Privilege Level**

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

**Related Documentation**

- Configuring the Local Password
- Configuring the PPP Password Authentication Protocol On a Physical Interface on page 124

### lockout

**Syntax**

```bash
lockout;
```

**Hierarchy Level**

-[edit interfaces interface-name sonet-options aps]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Switching Between the Working and Protect Circuits
log-prefix (Interfaces)

Syntax

log-prefix prefix-value;

Hierarchy Level

[edit interfaces interface-name services-options syslog host hostname]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Set the system logging prefix value.

Options

prefix-value—System logging prefix value.

Required Privilege

Level

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

Related Documentation

- Junos OS Services Interfaces Library for Routing Devices
- Configuring System Logging for Services Interfaces

logical-interface-fpc-redundancy (Aggregated Ethernet Subscriber Interfaces)

Syntax

logical-interface-fpc-redundancy;

Hierarchy Level

[edit interfaces ae number aggregated-ether-options]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2R2 for EX Series switches.

Description

Provide module redundancy for demux subscribers on aggregated Ethernet bundles configured with targeted distribution. Backup links for a subscriber are chosen on a different EQ DPC or MPC from the primary link, based on the link with the fewest number of subscribers among the links on different modules. If all links are on a single module when this is configured, backup links are not provisioned.

By default, link redundancy is provided for the aggregated Ethernet bundle.

Required Privilege

Level

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

Related Documentation

- Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface
- Configuring Module Redundancy for a Virtual Chassis
**logical-interface-policer**

**Syntax**

`logical-interface-policer;`

**Hierarchy Level**

- `[edit dynamic-profiles profile-name firewall policer policer-name]`
- `[edit dynamic-profiles profile-name firewall three-color-policer name]`
- `[edit firewall atm-policer atm-policer-name]`
- `[edit firewall policer policer-name]`
- `[edit firewall policer policer-template-name]`
- `[edit firewall three-color-policer policer-name]`
- `[edit logical-systems logical-system-name firewall policer policer-name]`
- `[edit logical-systems logical-system-name firewall three-color-policer name]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

Support at the `[edit firewall three-color-policer policer-name]` hierarchy level introduced in Junos OS Release 8.2.

Logical systems support introduced in Junos OS Release 9.3.

Support at the `[edit dynamic-profiles ... policer policer-name]` and `[edit dynamic-profiles ... three-color-policer name]` hierarchy levels introduced in Junos OS Release 11.4.

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Support for PTX series routers with third-generation FPCs added in Junos OS Release 18.3R1.

**Description**

Configure a logical interface policer. For PTX series routers running Junos OS Release 18.3R1 or later, you can use this command to configure separate firewall filters for different family address types (IPv4 and IPv6) that share the same interface, and configure the same policer as an action for the filter.

To configure the aggregate policer, configure the firewall policer you want to use as `logical-interface-policer`. And at the `firewall family family-name filter filter-name` hierarchy level where you will reference the policer, make the policer an `interface-specific` firewall filter action.

The sample configuration shows the relationship.

```plaintext
firewall {
    policer Shared_Policer {
        logical-interface-policer;
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 500k;
        }
        then {
            discard;
        }
    }
}
```
family inet {
  filter filter_name{
    interface-specific;
    term term_name {
      then {
        policer Shared_Policer;
        count cinet;
      }
    }
  }
}

NOTE: Starting in Junos OS Release 12.2R2, on T Series Core Routers only, you can configure an MPLS LSP policer for a specific LSP to be shared across different protocol family types. You must include the logical-interface-policer statement to do so.

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

Related Documentation
- Two-Color and Three-Color Logical Interface Policers
- Traffic Policer Types
- Configuring and Applying Tricolor Marking Policers
- action
- Configuring Gigabit Ethernet Two-Color and Tricolor Policers
- action on page 400
### logical-systems

**Syntax**

```
logical-systems {
  logical-system-name {
    ...logical-system-configuration...
  }
}
```

**Hierarchy Level**

[edit]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement name changed from `logical-routers` in Junos OS Release 9.3.

**Description**

Configure a logical system.

**Options**

- `logical-system-name`—Name of the logical system.

**Required Privilege Level**

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

**Related Documentation**

- *Logical Systems Feature Guide for Routers and Switches*
### long-buildout

**Syntax**  
(long-buildout | no-long-buildout);

**Hierarchy Level**  
[edit interfaces interface-name t3-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
Configure the T3 line buildout. A T3 interface has two settings for the T3 line buildout: a short setting, which is less than 255 feet (68 meters), and a long setting, which is greater than 255 feet and shorter than 450 feet (137 meters).

This statement applies to copper-cable-based T3 interfaces only. You cannot configure a line buildout for a DS3 channel on a channelized OC12 interface, which runs over fiber-optic cable.

**Default**  
A T3 interface uses the short line buildout setting (**no-long-buildout**) for wires shorter than 255 feet (68 meters).

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

**Related Documentation**  
- Configuring the T3 Line Buildout
loop-timing

Syntax  (loop-timing | no-loop-timing);

Hierarchy Level  [edit interfaces ct3-fpc/pic/port t3-options],
                 [edit interfaces e1-fpc/pic/port:0 sonet-options],
                 [edit interfaces stm1-fpc/pic/port sonet-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For channelized IQ interfaces and non-IQ channelized STMI interfaces only, configure
              the SONET/SDH or DS3-level clocking source.

NOTE: On M Series, MX Series, and T Series routers, under E1 channels, loop
timing can be configured only at channel 0. When you configure on channel
0, it is applicable on all channels as internal by default.

Options  loop-timing—Configure loop timing (external) clocking.
         no-loop-timing—Configure line timing (internal) clocking.
Default: no-loop-timing

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

Related Documentation  • Configuring Channelized IQ and IQE SONET/SDH Loop Timing
                       • Configuring the Channelized T3 Loop Timing
                       • clocking on page 472
**loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3)**

**Syntax**

```
loopback (local | payload | remote);
```

**Hierarchy Level**

```
[edit interfaces ce1-fpc/pic/port],
[edit interfaces ct1-fpc/pic/port],
[edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name ds0-options],
[edit interfaces interface-name dsl-options],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name e3-options],
[edit interfaces interface-name shdsl-options],
[edit interfaces interface-name sonet-options],
[edit interfaces interface-name t1-options],
[edit interfaces interface-name t3-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**

Configure a loopback connection. To turn off the loopback capability, remove the `loopback` statement from the configuration.

**NOTE:** When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the loopback statement must be included with the local or remote option at the `[edit interfaces ce1-fpc/pic/port]` or `[edit interfaces ct1-fpc/pic/port]` hierarchy level as appropriate.

When configuring T1 interfaces on 10-port Channelized E1/T1 IQE PICs, the loopback statement must be included with the payload option at the `[edit interfaces t1-fpc/pic/port]` hierarchy level.

**NOTE:** When configuring CE1 or CT1 interfaces on the 16-port Channelized E1/T1 MIC (MIC-3D-16CHE1-T1-CE), you must include the loopback statement at the `[edit interfaces ce1-fpc/pic/port]` hierarchy level, or `[edit interfaces ct1-fpc/pic/port]`.

To configure loopback on channelized IQ and IQE PICs, SONET/SDH level, use the `sonet-options loopback` statement local and remote options at the controller interface (coc48, cstm16, coc12, cstm4, coc3, cstm1). It is ignored for path-level interfaces `so-fpc/pic/port` or `so-fpc/pic/port:channel`. 
Options  

local—Loop packets, including both data and timing information, back on the local router’s PIC. NxDS0 IQ interfaces do not support local loopback.

payload—For channelized T3, T1, and NxDS0 IQ interfaces only, loop back data only (without clocking information) on the remote router’s PIC. With payload loopback, overhead is recalculated. Neither ATM-over-asymmetrical digital subscriber line (ADSL) interfaces nor ATM-over-SHDSL interfaces support payload loopback.

remote—Loop packets, including both data and timing information, back on the remote router’s interface card. NxDS0 IQ interfaces do not support remote loopback.

Required Privilege 

interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

Related Documentation 

- Configuring E3 and T3 Parameters on ATM Interfaces
- Configuring E1 Loopback Capability
- Configuring E3 Loopback Capability
- Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External
- Configuring SHDSL Operating Mode on an ATM Physical Interface
- Configuring T1 Loopback Capability
- Configuring T3 Loopback Capability
- feac-loop-respond on page 611
loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet)

Syntax
(loopback | no-loopback);

Hierarchy Level
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options],
[edit interfaces interface-range name ether-options]

For QFX Series and EX Series:
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name ether-options],

For SRX Series Devices and vSRX:
[edit interfaces interface-name redundant-ether-options]

Release Information
Statement introduced before Junos OS Release 7.4 for MX Series.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
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.
Statement modified in Junos OS Release 9.2 for the SRX Series.

Description
For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, enable or disable loopback mode.

NOTE:
- By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system.
- IPv6 Neighbor Discovery Protocol (NDP) addresses are not supported on Gigabit Ethernet interfaces when loopback mode is enabled on the interface. That is, if the loopback statement is configured at the [edit interfaces ge-fpc/pic/port gigether-options] hierarchy level, an NDP address cannot be configured at the [edit interfaces ge-fpc/pic/port unit logical-unit-number family inet6 address] hierarchy level.

Default
By default, loopback is disabled.
Required Privilege Level: interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

Related Documentation:
- Configuring Ethernet Loopback Capability
- Understanding Interfaces

**loopback (Serial)**

**Syntax**

```plaintext
loopback mode;
```

**Hierarchy Level**

```
[edit interfaces interface-name serial-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure a loopback connection.

**Default**

If you do not include this statement, there is no loopback connection.

**Options**

`mode`—You can specify the one of the following loopback modes:

- **dce-local**—For EIA-530 interfaces only, loop packets back on the local DCE.
- **dce-remote**—For EIA-530 interfaces only, loop packets back on the remote DCE.
- **local**—Loop packets back on the local router's PIC.
- **remote**—Loop packets back on the line interface unit (LIU).

**Required Privilege Level**

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

**Related Documentation**

- Configuring Serial Loopback Capability on page 328
loopback-clear-timer

Syntax

```
loopback-clear-timer seconds;
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number ppp-options],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]

Release Information

Statement introduced in Junos OS Release 8.5.

Description

For interfaces with PPP, PPP TCC, PPP over Ethernet, PPP over ATM, and PPP over Frame Relay encapsulations, configure a loop detection clear timer for the Link Control Protocol (LCP) component of a PPP session.

Options

seconds—The time in seconds to wait before the loop detection flag is cleared if it is not cleared by the protocol.

Range: 1 through 60 seconds

Default: 9 seconds

Required Privilege Level

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

Related Documentation

• Configuring the PPP Clear Loop Detected Timer on page 178
loss-priority

Syntax  
loss-priority (high | low);

Hierarchy Level  
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier premium forwarding-class class-name]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Specify the packet loss priority value.

Options  
high—Packet has high loss priority.

low—Packet has low loss priority.

Required Privilege  
interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

Related Documentation  
• Specifying an Output Priority Map
loss-threshold

Syntax  loss-threshold number;

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name continuity-check]

Release Information  Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport
Routers.

Description  Specify the number of continuity check messages lost before marking the remote MEP
as down. The value can be from 3 to 256 protocol data units (PDUs). The default value
is 3 PDUs.

Options  number—The number of continuity check messages that can be lost before the remote
MEP is considered down.

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

Related Documentation  •  Continuity Check Protocol Parameters Overview
•  Configuring Continuity Check Protocol Parameters for Fault Detection
**low-plp-max-threshold**

**Syntax**  
low-plp-max-threshold *percent*;

**Hierarchy Level**  
[edit interfaces at-fpc/pic/port atm-options linear-red-profiles *profile-name*]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For ATM2 IQ interfaces only, define the drop profile fill-level for the low PLP CoS VC. When the fill level exceeds the defined percentage, all packets are dropped.

**Options**  
*percent*—Fill-level percentage when linear RED is applied to cells with PLP.

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

**Related Documentation**  
- *ATM2 IQ VC Tunnel CoS Components Overview*  
- *high-plp-max-threshold* on page 641  
- *low-plp-threshold* on page 768  
- *Configuring Linear RED Profiles on ATM Interfaces*  
- *high-plp-max-threshold*  
- *queue-depth* on page 937
**low-plp-threshold**

**Syntax**

low-plp-threshold percent;

**Hierarchy Level**

[edit interfaces at-fpc/pic/port atm-options linear-red-profiles profile-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, define the CoS VC drop profile fill-level percentage when linear RED is applied to cells with low PLP. When the fill level exceeds the defined percentage, packets with low PLP are randomly dropped by RED. This statement is mandatory.

**Options**

`percent`—Fill-level percentage when linear RED is applied to cells with low PLP.

**Required Privilege Level**

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

**Related Documentation**

- ATM2 IQ VC Tunnel CoS Components Overview
- `high-plp-max-threshold` on page 641
- `high-plp-threshold` on page 637
- Configuring Linear RED Profiles on ATM Interfaces
- `high-plp-max-threshold`  
- `high-plp-threshold`  
- low-plp-max-threshold on page 767
- queue-depth on page 937
lowest-priority-defect

### Syntax

```
lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect | rem-err-xcon | xcon)
```

### Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name mep mep-id]
```

### Release Information

Statement introduced in Junos OS Release 10.0.

### Description

Specify the lowest priority defect that is allowed to generate a Fault Alarm whenever CFM detects a defect. This configuration is done at the MEP level.

### Options

Specify one of the following lowest priority defect options:

- **all-defects**—Allows all defects.
- **err-xcon**—Allows only erroneous CCM and cross-connect CCM defects.
- **mac-rem-err-xcon**—Allows only MAC, not receiving CCM, erroneous CCM, and cross-connect defects.
- **no-defect**—Allows no defects.
- **rem-err-xcon**—Allows only not receiving CCM, erroneous CCM, and cross-connect CCM defects.
- **xcon**—Allows only cross-connect CCM defects.

### Required Privilege Level

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

### Related Documentation

- [Configuring the Maintenance End Point Lowest Priority Defect](#)
lsq-failure-options

**Syntax**

```plaintext
lsq-failure-options {
    no-termination-request;
    [trigger-link-failure interface-name];
}
```

**Hierarchy Level**

```
[edit interfaces lsq-fpc/pic/port]
```

**Release Information**

Statement introduced in Junos OS Release 7.4.

**Description**

For AS PIC or MultiServices PIC link services IQ (lsq) interfaces only, define the failure recovery option settings.

**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**

- Junos OS Services Interfaces Library for Routing Devices
mac

Syntax  
mac mac-address;

Hierarchy Level  
[edit interfaces interface-name]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Set the MAC address of the interface. Use this statement at the [edit interfaces ... ps0] hierarchy level to configure the MAC address for a pseudowire logical device that is used for subscriber interfaces over point-to-point MPLS pseudowires.

Options  
mac-address—MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or nnnn:nnnn:nnnn:nnnn. For example, 0000.5e00.5355 or 00:00:5e:00:53:55.

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

Related Documentation  
• Configuring the MAC Address on the Management Ethernet Interface  
• Configuring a Pseudowire Subscriber Logical Interface Device
mac-address (Accept Source Mac)

Syntax  
mac-address mac-address policer;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number accept-source-mac],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number accept-source-mac ]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description  
For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), for Gigabit Ethernet DPCs on MX Series routers, and 100-Gigabit Ethernet Type 5 PIC with CFP, specify a remote MAC address on which to count incoming and outgoing packets.

Options  
mac-address—MAC address. Specify the MAC address as six hexadecimal bytes in one of the following formats: nnnn.nnnn.nnnn or nnnn:nnnn:nnnn:nnnn. For example, 0011.2233.4455 or 00:11:22:33:44:55.

policer—MAC policer. For more information, see policer (MAC).

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

Related Documentation  
• Configuring MAC Address Filtering
mac-address (VLAN and Stacked VLAN Interfaces)

**Syntax**
mac-address;

**Hierarchy Level**
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include],

**Release Information**
Statement introduced in Junos OS Release 10.0.

**Description**
Specify that the client hardware address (chaddr) from the incoming DHCP discover packet be concatenated with the username during the subscriber authentication process.

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

**Related Documentation**
- Configuring VLAN Interface Username Information for AAA Authentication
mac-learn-enable

Syntax

mac-learn-enable;

Hierarchy Level

[edit interfaces interface-name gigether-options ethernet-switch-profile]
[edit interfaces aex aggregated-ether-options ethernet-switch-profile]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), for Gigabit Ethernet DPCs on MX Series routers, for 100-Gigabit Ethernet Type 5 PIC with CFP, and for MPC3E, MPC4E, MPC5E, MPC5EQ, and MPC6E MPCs, configure dynamic learning of the source and destination MAC addresses. By default, the interface is not allowed to dynamically learn source and destination MAC addresses.

To disable dynamic learning of the source and destination MAC addresses after it has been configured, you must delete mac-learn-enable from the configuration.

MPCs support MAC address accounting for an individual interface or an aggregated Ethernet interface member link only after the interface has received traffic from the MAC source. If traffic is only exiting an interface, the MAC address is not learned and MAC address accounting does not occur.

Required Privilege Level

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

Related Documentation

• Configuring MAC Address Filtering
• Configuring MAC Address Accounting
mac-validate

Syntax
mac-validate (loose | strict);

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

Release Information
Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Enable IP and MAC address validation for static Ethernet and IP demux interfaces.

Options
loose—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.

strict—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple’s MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.

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

Related Documentation
• MAC Address Validation on Static Ethernet Interfaces Overview
• Configuring an IP Demultiplexing Interface on page 296
• Configuring a VLAN Demultiplexing Interface on page 301
### maintenance-association

**Syntax**

```
maintenance-association ma-name {
    short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
    protect-maintenance-association protect-ma-name;
    remote-maintenance-association remote-ma-name;
    continuity-check {
        hold-interval minutes;
        interval (10m | 10s | 1m | 1s | 100ms);
        loss-threshold number;
    }
    mep mep-id {
        auto-discovery;
        direction (up | down);
        interface interface-name (protect | working);
        lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
            rem-err-xcon | xcon);
        priority number;
        remote-mep mep-id {
            action-profile profile-name;
            sla-iterator-profile profile-name {
                data-tlv-size size;
                iteration-count count-value;
                priority priority-value;
            }
        }
    }
}
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

**Description**

Configure the name of the maintenance association in IEEE-compliant format.

**Options**

- **ma-name**—The name of the maintenance association within the maintenance domain.

  The remaining statements are explained separately. See CLI Explorer.

**Required Privilege**

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

**Related Documentation**

- Creating a Maintenance Association
- Configuring a MEP to Generate and Respond to CFM Protocol Messages
maintenance-domain

Syntax

```
maintenance-domain domain-name {
  bridge-domain name <vlan-id [ vlan-ids ]>
  instance vpls-instance-name
  level number
  maintenance-association ma-name {
    protect-maintenance-association protect-ma-name
    remote-maintenance-association remote-ma-name
    short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id)
    continuity-check {
      hold-interval minutes
      interval (10m | 10s | 1m | 1s | 100ms)
      loss-threshold number
    }
    mep mep-id {
      auto-discovery
      direction (up | down)
      interface interface-name (protect | working)
      lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect |
        rem-err-xcon | xcon)
      priority number
      remote-mep mep-id {
        action-profile profile-name
        sla-iterator-profile profile-name {
          data-tlv-size size
          iteration-count count-value
          priority priority-value
        }
      }
      mep-half-function (none | default | explicit)
      name-format (character-string | none | dns | mac+2oct)
    }
    virtual-switch name {
      bridge-domain name <vlan-id [ vlan-ids ]>
    }
  }
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Support for multiple down MEP introduced in Junos OS Release 15.1R1 for MX Series Routers.

Description

Configure the name of the maintenance domain in IEEE-compliant format.
NOTE: For MX Series Routers, you can configure multiple down MEPs for a single instance of maintenance domain identifier and maintenance association name to monitor services provided on Virtual Private LAN Service (VPLS), bridge, circuit cross-connect (CCC), and IPv4 domains.

Options  
**domain-name**—Name of the maintenance domain.

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**

- Creating a Maintenance Domain
- Configuring a MEP to Generate and Respond to CFM Protocol Messages

### master-only

**Syntax**

master-only;

**Hierarchy Level**

- [edit groups rex interfaces (fxp0 | em0) unit logical-unit-number family family address],
- [edit groups rex logical-systems logical-system-name interfaces fxp0 unit logical-unit-number family family address],
- [edit interfaces (fxp0 | em0) unit logical-unit-number family family address],
- [edit logical-systems logical-system-name interfaces fxp0 unit logical-unit-number family family address]

**Release Information**

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

**Description**

Configure the IP address to be used when the Routing Engine is the current master.

**Required Privilege**

**Level**

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

**Related Documentation**

- Configuring a Consistent Management IP Address
- CLI User Guide
maximum-contexts

Syntax  maximum-contexts number <force>;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number compression rtp],
     [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number compression rtp]

Release Information  Statement introduced in Junos OS Release 7.5.

Description  Specify the maximum number of RTP contexts to accept during negotiation.

Options  number—Maximum number of contexts.

          force—(Optional) Requires the PIC to use the value specified for maximum RTP contexts,
                  regardless of the negotiated value. This option allows the software to interoperate
                  with Junos OS Releases that base the RTP context value on link speed.

Required Privilege  interface—To view this statement in the configuration.

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

Related Documentation  •  Junos OS Services Interfaces Library for Routing Devices
**maximum-requests**

**Syntax**

```
maximum-requests times;
```

**Hierarchy Level**

```
[edit protocols dot1x authenticator interface interface-id]
```

**Release Information**

Statement introduced in Junos OS Release 9.3.

**Description**

Specify the maximum number of retransmission times of an EAPOL Request packet to the client before it times out the authentication session.

**Options**

- `times`—Specify the maximum number of retransmission times.
  
  **Range:** 1 through 10 times
  
  **Default:** 2 times

**Required Privilege Level**

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

**Related Documentation**

- [IEEE 802.1x Port-Based Network Access Control Overview](#)
- [authenticator on page 434](#)
- [dot1x on page 534](#)
- [interface (IEEE 802.1x) on page 687](#)
**maximum-vcs**

**Syntax**

```
maximum-vcs maximum-vcs;
```

**Hierarchy Level**

```
[edit interfaces at-fpc/pic/port atm-options vpi vpi-identifier]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM1 interfaces, configure the maximum number of virtual circuits (VCs) allowed on a virtual path (VP). When configuring ATM1 interfaces on the router, you must include this statement.

For a configured virtual path identifier (VPI), valid virtual channel identifier (VCI) numbers are from 0 through \((\text{maximum-vcs} \text{ value} - 1)\). VCI numbers 0 through 31 are reserved by the ATM Forum. It is recommended that you use a VCI number higher than 31 when connecting to an ATM switch.

**Options**

- **maximum-vcs**—Maximum number of VCs on the VP.
  - **Range:** 1 through 4090

**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 Number of ATM1 VCs on a VP
- multipoint-destination on page 807
- promiscuous-mode on page 927
- vci on page 1115

Copyright © 2019, Juniper Networks, Inc.
mc-ae

Syntax

```perl
mc-ae {
  chassis-id chassis-id;
  events {
    iccp-peer-down;
    force-icl-down;
    prefer-status-control-active;
  }
  init-delay-time seconds;
  mc-ae-id mc-ae-id;
  mode (active-active | active-standby);
  redundancy-group group-id;
  revert-time revert-time;
  status-control (active | standby);
  switchover-mode (non-revertive | revertive);
}
```

Hierarchy Level

- [edit interfaces aeX aggregated-ether-options],
- [edit logical-systems logical-system-name interfaces aeX aggregated-ether-options]

Release Information

Statement introduced in Junos OS Release 9.6 for MX Series routers.
- `events` statement introduced in Junos OS Release 11.4R4 for MX Series routers.
- Statement introduced in Junos OS Release 12.2 for the QFX Series. Only the `chassis-id`, `mc-ae-id`, `mode active-active`, and `status-control (active | standby)` options are supported on QFX Series devices.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
- `prefer-status-control-active` statement introduced in Junos OS Release 13.2R1 for EX Series switches.
- `init-delay-time seconds` statement introduced in Junos OS Release 13.2R3 for EX Series switches.
- `switchover-mode` and `revert-time` statements introduced in Junos OS Release 13.3.
- Support for logical systems introduced in Junos OS Release 14.1.

Description

Enable multichassis link aggregation groups (MC-LAG), which enables one device to form a logical LAG interface with two or more other devices.

Options

- **chassis-id**—Specify the chassis ID for Link Aggregation Control Protocol (LACP) to calculate the port number of MC-LAG physical member links.
  - **Values:** 0 or 1

- **events**—Specify an action if a specific MC-LAG event occurs.
  - `iccp-peer-down`—Specify an action if the ICCP peer of this node goes down.
  - `force-icl-down`—If the node's ICCP peer goes down, bring down the interchassis-link logical interface.
prefer-status-control-active—Specify that the node configured as status-control active become the active node if the peer of this node goes down.

When ICCP goes down, you can use this keyword to make a mc-lag PE to become the active PE. For example, if you want mc-lag PE1 to be Active on ICCP down, then configure this keyword in PE1. It is not recommended to configure this keyword in both the mc-lag PEs.

NOTE: The prefer-status-control-active statement can be configured with the status-control standby configuration to prevent the LACP MC-LAG system ID from reverting to the default LACP system ID on ICCP failure. Use this configuration only if you can ensure that ICCP will not go down unless the router or switch is down. You must also configure the hold-time down value (at the [edit interfaces interface-name] hierarchy level) for the interchassis link with the status-control standby configuration to be higher than the ICCP BFD timeout. This configuration prevents data traffic loss by ensuring that when the router or switch with the status-control active configuration goes down, the router or switch with the status-control standby configuration does not go into standby mode.

To make the prefer-status-control-active configuration work with the status-control standby configuration when an interchassis-link logical interface is configured on aggregate Ethernet interface, you must configure the lacp periodic interval statement at the [edit interface interface-name aggregated-ether-options] hierarchy level as slow or configure the detection-time threshold statement at the [edit protocols iccp peer liveness-detection] hierarchy level as less than 3 seconds.

init-delay-time seconds—To minimize traffic loss, specify the number of seconds in which to delay bringing the multichassis aggregated Ethernet interface back to the up state when you reboot an MC-LAG peer.

NOTE: On QFX and EX Series switches, the default session establishment hold time is 300 seconds. However, the session establishment time must be at least 100 seconds higher than the init delay time. You can optionally update the session establishment time to be 340 seconds and the init delay time to be 240 seconds.
**mc-ae-id mc-ae-id**—Specify the identification number of the MC-LAG device. The two MC-LAG network devices that manage a given MC-LAG must have the same identification number.

**Range:** 1 through 65,535

**mode (active-active | active-standby)**—Specify whether the MC-LAG is in active-active or active-standby mode.

**NOTE:** You can configure IPv4 (inet) and IPv6 (inet6) addresses on mc-ae interfaces when the active-standby mode is configured.

**redundancy-group group-id**—Specify the redundancy group identification number. The Inter-Chassis Control Protocol (ICCP) uses the redundancy group ID to associate multiple chassis that perform similar redundancy functions.

**Range:** 1 through 4,294,967,294

**revert-time**—Wait interval (in minutes) before the switchover to the preferred node is performed when the switchover-mode is configured as revertive.

**Range:** 1 through 10

**status-control (active | standby)**—Specify whether the chassis becomes active or remains in standby mode when an interchassis link failure occurs.

**switchover-mode (non-revertive | revertive)**—Specify whether Junos OS should trigger a link switchover to the preferred node when the active node is available.

**NOTE:** For revertive mode to automatically switch over to the preferred node, the status-control statement should be configured as active.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Interface—To view this statement in the configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Interface-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
member-interface-speed

Syntax:  member-interface-speed speed;

Hierarchy Level:  [edit interfaces container-options member-interface-type]


Description:  Specify container-interface member-interface speed options.

Options:  speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation:
- Displaying APS Using a Container Interface with ATM Encapsulation
- Configuring Container Interfaces for APS on SONET Links
- container-options on page 486
member-interface-type

Syntax  
```  
member-interface-type sonet [
  member-interface-speed [ speed ];
]  
```

Hierarchy Level  
[edit interfaces container-options]

Release Information  
Statement introduced in Junos OS Release 9.2.

Description  
Specify container-interface member-interface type as sonet and speed options.

Options  
- **sonet**—Protocol type of the container interface, specify sonet.
- **speed**—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation  
- Displaying APS Using a Container Interface with ATM Encapsulation
- Configuring Container Interfaces for APS on SONET Links
- container-options on page 486
mep

Syntax

```plaintext
mep mep-id [ action-profile action-profile-name
auto-discovery;
direction (up | down);
interface interface-name (protect | working);
priority number;
remote-mep mep-id [ action-profile profile-name;
sla-iterator-profile profile-name {
data-tlv-size size;
iteration-count count-value;
priority priority-value;
}
}
]
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  md-name maintenance-association ma-name]
```

Release Information
Statement introduced in Junos OS Release 8.4.

Description
The numeric identifier of the maintenance association end point (MEP) within the maintenance association.

Options

- **mep mep-id**—Specify the numeric identifier of the MEP.

  Range: 1 through 8191

  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

- Ethernet Alarm Indication Signal (ETH-AIS) Function Overview
- Configuring ETH-AIS on a CFM MEP
- Configuring a MEP to Generate and Respond to CFM Protocol Messages
**minimum-links**

**Syntax (SRX, MX, T, M, EX, QFX Series, EX4600, Qfabric System)**

minimum-links number;

**Hierarchy Level (EX Series)**

[edit interfaces aex aggregated-ether-options].
[edit interfaces aex aggregated-sonet-options].
[edit interfaces interface-name mfr-uni-nni-bundle-options].
[edit interfaces interface-name unit logical-unit-number].
[edit interfaces interface-range range aggregated-ether-options].
[edit interfaces interface-range range aggregated-sonet-options].
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number].

**Hierarchy Level (QFX Series)**

[edit interfaces aex aggregated-ether-options]

**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**

For aggregated Ethernet, SONET/SDH, multilink, link services, and voice services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up.

**Options**

*number*—Number of links.

**Range:** On M120, M320, MX Series, T Series, and TX Matrix routers with Ethernet interfaces, the valid range for minimum-links number is 1 through 64. When the maximum value (16) is specified, all configured links of a bundle must be up for the bundle to be labeled up. On all other routers and on EX Series switches, other than EX8200 switches, the range of valid values for minimum-links number is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled up. On EX8200 switches, the range of valid values for minimum-links number is 1 through 12. When the maximum value (12) is specified, all configured links of a bundle must be up for the bundle to be labeled up. On EX4600, QFX Series and Q Fabric Systems, the range of valid values for minimum-links number is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled up.

**Default:** 1

**Required Privilege Level**

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

**Related Documentation**

- Configuring Aggregated Ethernet Minimum Links
- Configuring Aggregated SONET/SDH Interfaces
• Configuring Aggregated Ethernet Links (CLI Procedure)
• Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
• Junos OS Services Interfaces Library for Routing Devices
• Configuring Link Aggregation

mip-half-function

Syntax

mip-half-function (none | default | explicit);

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name],
[edit protocols oam ethernet connectivity-fault-management maintenance-association ma-name]

Release Information


Description

Specify the OAM Ethernet CFM maintenance domain MIP half functions.

NOTE: Whenever a MIP is configured and a bridge domain is mapped to multiple maintenance domains or maintenance associations, it is essential that the mip-half-function value for all maintenance domains and maintenance associations are the same.

Options

none—Specify to not use the mip-half-function.

default—Specify to use the default mip-half-function.

explicit—Specify an explicit mip-half-function.

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

• Creating a Maintenance Domain

• maintenance-domain on page 777
**mlfr-uni-nni-bundle-options**

**Syntax**
```
mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu | c-lmi);
    minimum-links number;
    mru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 seconds;
    t392 number;
    yellow-differential-delay milliseconds;
}
```

**Hierarchy Level**
```
[edit interfaces interface-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Configure link services and voice services interface management properties.

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 Frame Relay Keepalives
- lmi (Frame Relay) on page 746
- lmi-type on page 749
- Junos OS Services Interfaces Library for Routing Devices
# mode (Dynamic Profiles)

**Syntax**

```plaintext
mode loose;
```

**Hierarchy Level**

```plaintext
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family (inet) rpf-check]
```

**Release Information**


**Description**

Check whether the packet has a source address with a corresponding prefix in the routing table. If a corresponding prefix is not found, unicast reverse path forwarding (RPF) loose mode does not accept the packet. Unlike strict mode, loose mode does not check whether the interface expects to receive a packet with a specific source address prefix.

**Default**

If you do not include this statement, unicast RPF is in strict mode.

**Required Privilege Level**

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

**Related Documentation**

- Configuring Unicast RPF Strict Mode on page 229
- Unicast RPF in Dynamic Profiles for Subscriber Interfaces
mode (Interfaces)

Syntax  
mode loose;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number family (inet | inet6) rpf-check],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family (inet | inet6) rpf-check]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 15.1F6 for PTX Series routers with third-generations FPCs installed.

Description  
Check whether the packet has a source address with a corresponding prefix in the routing table. If a corresponding prefix is not found, unicast reverse path forwarding (RPF) loose mode does not accept the packet. Unlike strict mode, loose mode does not check whether the interface expects to receive a packet with a specific source address prefix.

Default  
If you do not include this statement, unicast RPF is in strict mode.

Required Privilege  
level

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

Related Documentation  
• Configuring Unicast RPF Strict Mode on page 229
**modem-options**

**Syntax**

```plaintext
modem-options {
  dialin (console | routable);
  init-command-string initialization-command-string;
}
```

**Hierarchy Level**

[edit interfaces umd0]

**Release Information**

Statement introduced in Junos OS Release 8.2.

**Description**

For J Series Services Routers, configure a USB port to act as a USB modem.

The remaining statement is 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**

- Specifying a USB Modem Interface on J Series Routers on page 331
monitor-session

Syntax  

```
monitor-session (interface-name | all);
```

Hierarchy Level  

[edit protocols ppp]

Release Information  
Statement introduced in Junos OS Release 7.5.

Description  
Monitor PPP packet exchanges. When monitoring is enabled, packets exchanged during a session are logged to the default log of /var/log/pppd.

Default  
If you do not include this statement, no PPPD-specific monitoring operations are performed.

Options  
all—Monitor PPP packet exchanges on all sessions.

```
interface-name—Logical interface name on which to enable session monitoring.
```

Required Privilege Level  
interface—To view this statement in the configuration.

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

Related Documentation  
- Monitoring a PPP Session on page 136
**mpls (Interfaces)**

**Syntax**

```plaintext
mpls {
  pop-all-labels {
    required-depth number;
  }
}
```

**Hierarchy Level**

- `[edit interfaces interface-name atm-options]`
- `[edit interfaces interface-name sonet-options]`
- `[edit interfaces interface-name fastether-options]`
- `[edit interfaces interface-name gigether-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For passive monitoring on ATM and SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode, process incoming IP packets that have MPLS labels.

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**

- *Removing MPLS Labels from Incoming Packets*
- *Enabling Packet Flow Monitoring on SONET/SDH Interfaces*
- *Junos OS Services Interfaces Library for Routing Devices*
mrru

Syntax    mrru bytes;

Hierarchy Level    [edit interfaces interface-name mfr-unl-nni-bundle-options],
    [edit interfaces interface-name unit logical-unit-number],
    [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information    Statement introduced before Junos OS Release 7.4.

Description    For multilink, link services, voice services, and J Series Services Routers ISDN interfaces only, set the maximum received reconstructed unit (MRRU). The MRRU is similar to the MTU, but is specific to multilink interfaces.

Options    bytes—MRRU size.
    Range: 1500 through 4500 bytes
    Default: 1500 bytes

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

Related Documentation    • mtu on page 797
    • Junos OS Services Interfaces Library for Routing Devices
### mtu

**Syntax**

```mtu bytes;```

**Hierarchy Level**

- `[edit interfaces interface-name]`
- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit interfaces interface-range name]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name protocols l2circuit local-switching interface interface-name backup-neighbor address]`
- `[edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name]`
- `[edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name backup-neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols vpls]`
- `[edit protocols l2circuit local-switching interface interface-name backup-neighbor address]`
- `[edit protocols l2circuit neighbor address interface interface-name]`
- `[edit protocols l2circuit neighbor address interface interface-name backup-neighbor address]`
- `[edit routing-instances routing-instance-name protocols l2vpn interface interface-name]`
- `[edit routing-instances routing-instance-name protocols vpls]`
- `[edit logical-systems name protocols ospf area name interface]`
- `[edit logical-systems name routing-instances name protocols ospf area name interface]`
- `[edit protocols ospf area name interface ]`
- `[edit routing-instances name protocols ospf area name interface ]`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for Layer 2 VPNs and VPLS introduced in Junos OS Release 10.4.
- Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
- Support at the `[set interfaces interface-name unit logical-unit-number family ccc]` hierarchy level introduced in Junos OS Release 12.3R3 for MX Series routers.
- Statement introduced in Junos OS 17.3R1 Release for MX Series Routers.

**Description**

Specify the maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

To route jumbo data packets on an integrated routing and bridging (IRB) interface or routed VLAN interface (RVI) on EX Series switches, you must configure the jumbo MTU size on the member physical interfaces of the VLAN that you have associated with the IRB interface or RVI, as well as on the IRB interface or RVI itself (the interface named irb or vlan, respectively).
CAUTION: For EX Series switches, setting or deleting the jumbo MTU size on an IRB interface or RVI while the switch is transmitting packets might cause packets to be dropped.

NOTE: The MTU for an IRB interface is calculated by removing the Ethernet header overhead \( [6(DMAC)+6(SMAC)+2(EtherType)] \). Because, the MTU is the lower value of the MTU configured on the IRB interface and the MTU configured on the IRB's associated bridge domain IFDs or IFLs, the IRB MTU is calculated as follows:

- In case of Layer 2 IFL configured with the flexible-vlan-tagging statement, the IRB MTU is calculated by including 8 bytes overhead (SVLAN+CVLAN).
- In case of Layer 2 IFL configured with the vlan-tagging statement, the IRB MTU is calculated by including a single VLAN 4 bytes overhead.
NOTE:

- If a packet whose size is larger than the configured MTU size is received on the receiving interface, the packet is eventually dropped. The value considered for MRU (maximum receive unit) size is also the same as the MTU size configured on that interface.

- Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values. You cannot configure an MTU for management Ethernet interfaces (fxp0, em0, or me0) or for loopback, multilink, and multicast tunnel devices.

- On ACX Series routers, you can configure the protocol MTU by including the mtu statement at the [edit interfaces interface-name unit logical-unit-number family inet] or [edit interfaces interface-name unit logical-unit-number family inet6] hierarchy level.
  - If you configure the protocol MTU at any of these hierarchy levels, the configured value is applied to all families that are configured on the logical interface.
  - If you are configuring the protocol MTU for both inet and inet6 families on the same logical interface, you must configure the same value for both the families. It is not recommended to configure different MTU size values for inet and inet6 families that are configured on the same logical interface.

- Starting in Release 14.2, MTU for IRB interfaces is calculated by removing the Ethernet header overhead (6(DMAC)+6(SMAC)+2(EtherType)), and the MTU is a minimum of the two values:
  - Configured MTU
  - Associated bridge domain's physical or logical interface MTU
    - For Layer 2 logical interfaces configured with flexible-vlan-tagging, IRB MTU is calculated by including 8 bytes overhead (SVLAN+CVLAN).
    - For Layer 2 logical interfaces configured with vlan-tagging, IRB MTU is calculated by including single VLAN 4 bytes overhead.

NOTE: Changing the Layer 2 logical interface option from vlan-tagging to flexible-vlan-tagging or vice versa adjusts the logical interface MTU by 4 bytes with the existing MTU size. As a result, the Layer 2 logical interface is deleted and re-added, and the IRB MTU is re-computed appropriately.
For more information about configuring MTU for specific interfaces and router or switch combinations, see "Configuring the Media MTU" on page 99.

**Options**

**bytes**—MTU size.

**Range:** 256 through 9192 bytes, 256 through 9216 (EX Series switch interfaces), 256 through 9500 bytes (Junos OS 12.1X48R2 for PTX Series routers), 256 through 9500 bytes (Junos OS 16.1R1 for MX Series routers)

---

**NOTE:** Starting in Junos OS Release 16.1R1, the MTU size for a media or protocol is increased from 9192 to 9500 for Ethernet interfaces on the following MX Series MPCs:

- MPC1
- MPC2
- MPC2E
- MPC3E
- MPC4E
- MPC5E
- MPC6E

**Default:** 1500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS), 1514 bytes (EX Series switch interfaces)

**Required Privilege Level**

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

**Related Documentation**

- Configuring the Media MTU on page 99
- Configuring the MTU for Layer 2 Interfaces
- Setting the Protocol MTU on page 209
multi-chassis-protection

Syntax
multi-chassis-protection {
  peer a.b.c.d {
    interface interface-name;
  }
}

Hierarchy Level [edit interfaces interface-name]


Description For MX Series routers with multichassis aggregated Ethernet (MC-AE) interfaces, you can use this statement under the physical interface level to reduce the configuration at the logical interface level if the following assumption exists:

If there are n + 1 logical interfaces under ae0, from ae0.0 through ae0.n, there will be n + 1 logical interfaces under ge-0/0/0 as well, from ge-0/0/0.0 through ge-0/0/0.n, and each ge-0/0/0 logical interface will be a protection link for the ae0 logical interface.

NOTE: A bridge domain cannot have MC-AE logical interfaces which belong to different redundancy groups.

If the Inter-Chassis Control Protocol (ICCP) connection is UP and the interchassis data link (ICL) comes UP, the router configured as standby will bring up the MC-AE interfaces shared with the peer.

The remaining statements are explained separately. See CLI Explorer.

Options
interface interface-name—Specify the interface: interface interface-name-fpc/pic/port

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

Related Documentation
• Configuring Multichassis Link Aggregation on MX Series Routers
• Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers and QFX Series Switches
• Configuring Aggregated Ethernet Link Protection
• Example: Configuring Aggregated Ethernet Link Protection
• peer on page 881
multicast-dlci

Syntax

multicast-dlci dlci-identifier;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For point-to-multipoint Frame Relay, link services, and voice services interfaces only, enable multicast support on the interface. You can configure multicast support on the interface if the Frame Relay switch performs multicast replication.

Options

dlci-identifier—DLCI identifier, a number from 16 through 1022 that defines the Frame Relay DLCI over which the switch expects to receive multicast packets for replication.

Required Privilege

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

Related Documentation

• Configuring a Multicast-Capable Frame Relay Connection
• dlci on page 531
• multipoint-destination on page 807
• Junos OS Services Interfaces Library for Routing Devices
**multicast-only**

Syntax: `multicast-only;`

Hierarchy Level: `[edit interfaces interface-name unit logical-unit-number family inet],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]`

Release Information: Statement introduced before Junos OS Release 7.4.

Description: Configure the unit and family so that it can transmit and receive multicast traffic only.
You can configure this property on the IP family only.

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

Related Documentation:
- Configuring the Protocol Family on page 190
- *Junos OS Services Interfaces Library for Routing Devices*
- `tunnel` on page 1087
multicast-statistics

Syntax multicast-statistics;

Hierarchy Level [edit interfaces interface-name]

Release Information Statement introduced before Junos OS Release 10.2.

Description For Ethernet, SONET, aggregated Ethernet, and aggregated SONET interfaces in T Series or TX Matrix routers, specify support for multicast statistics on a physical interface to enable multicast accounting for all the logical interfaces below the physical interface.

Default not enabled—must be configured to enable

Required Privilege Level

Required Privilege Level

Related Documentation

• Configuring Multicast Statistics Collection on Aggregated Ethernet Interfaces
• Configuring Multicast Statistics Collection on Aggregated SONET Interfaces
• Configuring Multicast Statistics Collection on Ethernet Interfaces
• Configuring Multicast Statistics Collection on SONET Interfaces
multicast-vci

Syntax: multicast-vci vpi-identifier.vci-identifier;

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

Release Information: Statement introduced before Junos OS Release 7.4.

Description: For ATM encapsulation only, and for point-to-multipoint ATM logical interfaces only, enable the support of multicast on the interface. You can configure multicast support on the interface if the ATM switch performs multicast replication.

Options:
- vci-identifier—ATM virtual circuit identifier.
  Range: 0 through 16,384
- vpi-identifier—ATM virtual path identifier.
  Range: 0 through 255
  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 a Multicast- Capable ATM1 or ATM2 IQ Connection
- multipoint-destination on page 807
- vci on page 1115
**multilink-max-classes**

**Syntax**
```
multilink-max-classes number;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For Adaptive Services (AS) PIC link services IQ interfaces (lsq) only, configure the number of multilink classes to be negotiated when a link joins the bundle.

**Options**
- `number`—The number of multilink classes to be negotiated when a link joins the bundle.
  - **Range:** 1 through 8
  - **Default:** None

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**
- Junos OS Services Interfaces Library for Routing Devices
- multipoint on page 806

**multipoint**

**Syntax**
```
multipoint;
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Configure the interface unit as a multipoint connection.

**Default**
If you omit this statement, the interface unit is configured as a point-to-point connection.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**
- Configuring a Multipoint Connection on page 177
- point-to-point on page 890
multipoint-destination

Syntax multipoint-destination address dlci dlci-identifier;
multipoint-destination address {
  epd-threshold cells;
  inverse-arp;
  oam-liveness {
    down-count cells;
    up-count cells;
  }
  oam-period (disable | seconds);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
    queue-length number;
  }
  vci vpi-identifier.vci-identifier;
}

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For point-to-multipoint Frame Relay or ATM interfaces only, enable the support of multicast on the interface. You can configure multicast support on the interface if the Frame Relay or ATM switch performs multicast replication.

Options address—Address of the remote side of the point-to-multipoint connection.

dlci-identifier—For Frame Relay interfaces, the data-link connection identifier.
Range: 0 through 0xFFFFFF (24 bits)

vci-identifier—For ATM interfaces, the virtual circuit identifier.
Range: 0 through 16,384

vpi-identifier—For ATM interfaces, the virtual path identifier.
Range: 0 through 255
Default: 0

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 a Point-to-Point ATM1 or ATM2 IQ Connection
• Configuring a Point-to-Multipoint Frame Relay Connection
• dlici on page 531
• encapsulation (Logical Interface) on page 567

**multiservice-options**

**Syntax**
```
multiservice-options {
  (syslog | no-syslog);
  (core-dump | no-core-dump);
  (dump-on-flow-control);
  flow-control-options {
    down-on-flow-control;
    dump-on-flow-control;
    reset-on-flow-control;
  }
}
```

**Hierarchy Level**
```
[edit interfaces mo-fpc/pic/port]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For monitoring services interfaces only, configure multiservice-specific interface properties.

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 Multiservice Physical Interface Properties on page 154
• Junos OS Services Interfaces Library for Routing Devices
• passive-monitor-mode on page 874
Syntax  n391 number;

Hierarchy Level  [edit interfaces interface-name mlfr-uni-nni-bundle-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For link services and voice services interfaces only, set the Frame Relay full status polling interval.

Options  number—Polling interval.
  Range: 1 through 255
  Default: 6

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

Related Documentation  • Junos OS Services Interfaces Library for Routing Devices
  • n392 on page 810
  • n393 on page 811
  • timeslots on page 1050
  • t392 on page 1040
**n392**

**Syntax**  
\[ \text{n392 number;} \]

**Hierarchy Level**  
[edit interfaces interface-name mfr-uni-nni-bundle-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For link services and voices interfaces only, set the Frame Relay error threshold, in number of errors.

**Options**  
- \text{number}—Error threshold.  
  - **Range:** 1 through 10  
  - **Default:** 3

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

**Related Documentation**  
- Junos OS Services Interfaces Library for Routing Devices  
- n391 on page 809  
- n393 on page 811  
- timeslots on page 1050  
- t392 on page 1040
Syntax  n393 number;

Hierarchy Level  [edit interfaces interface-name mfr-uni-nni-bundle-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For link services and voices interfaces only, set the Frame Relay monitored event count.

Options  number—Number of event count.
Range:  1 through 10
Default:  4

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

Related Documentation  • Junos OS Services Interfaces Library for Routing Devices
• n391 on page 809
• n392 on page 810
• timeslots on page 1050
• t392 on page 1040
name-format

Syntax

```latex
name-format (character-string | none | dns | mac+2oct);
```

Hierarchy Level

```latex
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
```

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

Description

Specify the format of the maintenance domain name.

Options

- **character-string**—The name is an ASCII character string.
- **none**—The maintenance domain name is not used.
- **dns**—The name is in domain name service (DNS) format. For example: www.juniper.net.
- **mac+2oct**—Name is the MAC address plus a two-octet maintenance association identifier. For example: 08:00:22:33:44:55.100.

Default: character-string

Required Privilege Level

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

Related Documentation

- Creating a Maintenance Association
- Creating a Maintenance Domain
native-vlan-id

Syntax
native-vlan-id vlan-id;

Hierarchy Level (QFX Series and EX4600)
For platforms without ELS:
[edit interfaces (QFX Series) interface-name unit 0 family ethernet-switching]
For platforms with ELS:
[edit interfaces (QFX Series) interface-name]

Hierarchy Level (ACX Series, EX Series, SRX Series, M Series, MX Series, and T Series)
[edit interfaces ge-fpc/pic/port],
[edit interfaces interface-name]

Hierarchy Level (SRX Series)
[edit interfaces interface-name]

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 9.5 for SRX Series.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

Description
Configure the VLAN identifier to associate with untagged packets received on the physical interface of a trunk mode interface for the following:

- QFX Series and EX4600
- M Series routers with Gigabit Ethernet IQ PICs with SFP and Gigabit Ethernet IQ2 PICs with SFP configured for 802.1Q flexible VLAN tagging
- MX Series routers with Gigabit Ethernet DPCs and MICs, Tri-Rate Ethernet DPCs and MICs, and 10-Gigabit Ethernet DPCs and MICs and MPCs configured for 802.1Q flexible VLAN tagging
- T4000 routers with 100-Gigabit Ethernet Type 5 PIC with CFP
- EX Series switches with Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces

The logical interface on which untagged packets are received must be configured with the same VLAN ID as the native VLAN ID configured on the physical interface, otherwise the untagged packets are dropped. To configure the logical interface, include the `vlan-id`
statement (matching the `native-vlan-id` statement on the physical interface) at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

When the `native-vlan-id` statement is included with the `flexible-vlan-tagging` statement, untagged packets are accepted on the same mixed VLAN-tagged port and on the interfaces that are configured for Q-in-Q tunneling.

When the `native-vlan-id` statement is combined with the `interface-mode` statement, untagged packets are accepted and forwarded within the bridge domain or VLAN that is configured with the matching VLAN ID.

To configure the logical interface, include the `vlan-id` statement (matching the `native-vlan-id` statement on the physical interface) at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

---

**NOTE:** Starting in Junos OS Release 17.1R1, you can send untagged traffic without a native VLAN ID to the remote end of the network. To do this, remove the native VLAN ID from the untagged traffic configuration by setting the `no-native-vlan-insert` statement. If you do not configure this statement, the native VLAN ID is added to the untagged traffic.

---

**Default**

By default, the untagged packets are dropped. That is, if you do not configure the `native-vlan-id` option, the untagged packets are dropped.

**Options**

- `vlan-id`—Numeric identifier of the VLAN.
  - **Range:** 1 through 4094

- `number`—VLAN ID number.
  - **Range:** (ACX Series routers, SRX Series devices and EX Series switches) 0 through 4094

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure)
- Understanding Bridging and VLANs on Switches
- Enabling VLAN Tagging
- Configuring Access Mode on a Logical Interface
- Configuring the Native VLAN Identifier on Switches With ELS Support
- Understanding Interfaces
- Understanding Q-in-Q Tunneling and VLAN Translation
- no-native-vlan-insert
- Sending Untagged Traffic Without VLAN ID to Remote End
- show ethernet-switching interfaces
- show vlans
- flexible-vlan-tagging on page 617
- Junos OS Network Interfaces Configuration Guide

ncp-max-conf-req

Syntax  ncp-max-conf-req number

Hierarchy Level  [edit interfaces so-fpc/pic/port unit number ppp-options]


Description  Set the maximum number of NCP Configure-Requests to be sent, after which the router goes to NCP down state.

Options  

number—Ranges from 0 to 65535, where 0 means send infinite NCP Configure-Requests and any other value specifies the maximum number NCP Configure-Requests to send and then stop sending.

Default—254

Range: 0 through 65,535

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

- Configuring the NCP Configure-Request Maximum Sent on page 179
- ppp-options on page 910
ncp-restart-timer

Syntax
ncp-restart-timer milliseconds;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number ppp-options],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]

Release Information
Statement introduced in Junos OS Release 8.1.

Description
For interfaces with PPP and PPP TCC encapsulations and on multilink PPP bundle interfaces, configure a restart timer for the Network Control Protocol (NCP) component of a PPP session.

Options
milliseconds—The time in milliseconds between successive NCP configuration requests.
Range: 500 through 10,000 milliseconds
Default: 3 seconds

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

Related Documentation
• Configuring the PPP Restart Timers on page 177
**nd6-stale-time**

**Syntax**

```
nd6-stale-time seconds;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family inet6]
```

**Release Information**


**Description**

Set the stale timer for IPv6 neighbor reachability confirmation. Reachability of the IPv6 neighbors is confirmed only after the stale timer has expired. For example, by setting the stale timer to 180 seconds, users can specify that IPv6 neighbor reachability be confirmed every 180 seconds.

**NOTE:** When the Routing Engine sends a control packet to an IPv6 neighbor, the stale timer is the maximum interval in which neighbor reachability is confirmed. In such cases, IPv6 neighbor reachability is confirmed before the stale timer expires.

**Default**

Default is 20 minutes (1200 seconds)

**Options**

`seconds`—Duration in seconds.

**Range:** 1 to 18000

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- IPv6 Neighbor Discovery Overview
- show ipv6 neighbors on page 2039
negotiate-address

Syntax

negotiate-address;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For interfaces with PPP encapsulation, enable the interface to be assigned an IP address by the remote end.

Required Privilege Level

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

Related Documentation

• Configuring IPCP Options for Interfaces with PPP Encapsulation on page 200
• address on page 407
• unnumbered-address (PPP) on page 1108
• Junos OS Administration Library
negotiation-options

Syntax

    negotiation-options {
        allow-remote-loopback;
        no-allow-link-events;
    }

Hierarchy Level

    [edit protocols oam link-fault-management interface interface-name]

Release Information

    Statement introduced in Junos OS Release 8.4.

Description

    Enable and disable IEEE 802.3ah Operation, Administration, and Management (OAM) features for Ethernet interfaces.

    The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

    • IEEE 802.3ah OAM Link-Fault Management Overview
neighbor (Automatic Protection Switching for SONET/SDH)

Syntax
neighbor address;

Hierarchy Level
[edit interfaces interface-name sonet-options aps]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
If you are configuring one router to be the working router and a second to be the protect router, configure the address of the remote interface. You configure this on one or both of the interfaces.

The address you specify for the neighbor must never be routed through the interface on which APS is configured, or instability will result. We strongly recommend that you directly connect the working and protect routers and that you configure the interface address of this shared network as the neighbor address.

Options
address—Neighbor’s address.

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

Related Documentation
• Configuring Basic Automatic Protect Switching

no-allow-link-events

Syntax
no-allow-link-events;

Hierarchy Level
[edit protocols oam ethernet link-fault-management interface interface-name negotiation-options]

Release Information
Statement introduced in Junos OS Release 8.4.

Description
Disable the sending of link event TLVs.

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

Related Documentation
• Disabling the Sending of Link Event TLVs
no-aggregate-delegate-processing

<table>
<thead>
<tr>
<th>Syntax</th>
<th>no-aggregate-delegate-processing;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit protocols oam ethernet connectivity-fault-management]</td>
</tr>
<tr>
<td>Description</td>
<td>Disable distribution of connectivity fault management (CFM) sessions on aggregated Ethernet interfaces.</td>
</tr>
<tr>
<td>Default</td>
<td>CFM sessions on aggregated Ethernet interfaces are distributed by default.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>Configure—To enter configuration mode. Control—To modify any configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>IEEE 802.1ag OAM Connectivity Fault Management Overview</td>
</tr>
</tbody>
</table>
**asynchronous-notification**

**Syntax**

(asynchronous-notification | no-asynchronous-notification);

**Hierarchy Level**

[edit interfaces ge-fpc/pic/port gigether-options ]

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

**Description**

(MX Series routers, T Series routers) For all Gigabit Ethernet interfaces (1-Gigabit, 10-Gigabit, and 100-Gigabit), configure support for notification of link down alarm generation and transfer.

(M120 and M320 routers) For all 10-Gigabit Ethernet PIC interfaces, configure support for notification of link down alarm generation and transfer.

- **asynchronous-notification**—Support notification of link down alarm generation and transfer.
- **no-asynchronous-notification**—Prohibit notification of link down alarm generation and transfer.

**Default**

Support for notification of link down alarm generation and transfer is not enabled.

**Required Privilege Level**

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

**Related Documentation**

- Gigabit Ethernet Notification of Link Down Alarm Overview
- Configuring Gigabit Ethernet Notification of Link Down Alarm
no-auto-mdix

Syntax  no-auto-mdix;

Hierarchy Level  [edit interface ge-fpc/port/pic gigether-options]

Release Information  Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description  Disable the Auto MDI/MDIX feature.

MX Series routers with Gigabit Ethernet interfaces automatically detect MDI and MDIX port connections. Use this statement to override the default setting. Remove this statement to return to the default setting.

Default  Auto MDI/MDIX is enabled by default.

Options  There are no options for this statement.

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

Related Documentation  • Ethernet Interfaces Overview
• gigether-options on page 632.
auto-negotiation

Syntax    (auto-negotiation | no-auto-negotiation) <remote-fault (local-interface-online | local-interface-offline)>;

Hierarchy Level    [edit interfaces interface-name ether-options],
                    [edit interfaces interface-name gigether-options],
                    [edit interfaces ge-pim/0/0 switch-options switch-port port-number]

Release Information    Statement introduced in Junos OS Release 7.6.
                        Statement introduced in Junos OS Release 9.0 for EX Series switches.
                        Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description    For Gigabit Ethernet interfaces on M Series, MX Series, T Series, TX Matrix routers, and
                ACX Series routers explicitly enable autonegotiation and remote fault. For EX Series
                switches, explicitly enable autonegotiation only.

                • auto-negotiation—Enables autonegotiation. This is the default.
                • no-auto-negotiation—Disable autonegotiation. When autonegotiation is disabled, you
                  must explicitly configure the link mode and speed.

                When you configure Tri-Rate Ethernet copper interfaces to operate at 1 Gbps,
                autonegotiation must be enabled.

                NOTE: On EX Series switches, an interface configuration that disables
                autonegotiation and manually sets the link speed to 1 Gbps is accepted when
                you commit the configuration; however, if the interface you are configuring
                is a Tri-Rate Ethernet copper interface, the configuration is ignored as invalid
                and autonegotiation is enabled by default.

                To correct the invalid configuration and disable autonegotiation:

                1. Delete the no-auto-negotiation statement and commit the configuration.

                2. Set the link speed to 10 or 100 Mbps, set no-auto-negotiation, and commit
                   the configuration.

                On EX Series switches, if the link speed and duplex mode are also configured, the
                interfaces use the values configured as the desired values in the negotiation. If
                autonegotiation is disabled, the link speed and link mode must be configured.

                NOTE: On T4000 routers, the auto-negotiation command is ignored for
                interfaces other than Gigabit Ethernet.
NOTE: On ACX Series routers, when you configure fiber interfaces (fiber media mode) to operate at 1 Gbps, autonegotiation is enabled by default to negotiate the speed and duplex settings. You can disable autonegotiation by using the (no-auto-negotiation) statement, and commit the configuration. In the fiber media mode. In copper interfaces (copper media mode), autonegotiation is enabled by default. To disable autonegotiation, you need to explicitly configure the link speed to 10 or 100 Mbps, set no-auto-negotiation, and commit the configuration.

Default  Autonegotiation is automatically enabled. No explicit action is taken after the autonegotiation is complete or if the negotiation fails.

Options  remote-fault (local-interface-online | local-interface-offline)—(Optional) For M Series, MX Series, T Series, TX Matrix routers, and ACX Series routers only, manually configure remote fault on an interface.

Default: local-interface-online

Required Privilege Level  interface—To view this statement in the configuration.

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

Related Documentation  • Gigabit Ethernet Autonegotiation Overview
  • Configuring Gigabit Ethernet Interfaces (CLI Procedure)
  • Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support
cbit-parity

Syntax  (cbit-parity | no-cbit-parity);

Hierarchy Level  [edit interfaces interface-name t3-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For T3 interfaces only, enable or disable C-bit parity mode, which controls the type of framing that is present on the transmitted T3 signal. When C-bit parity mode is enabled, the C-bit positions are used for the far-end block error (FEBE), far-end alarm and control (FEAC), terminal data link, path parity, and mode indicator bits, as defined in ANSI T1.107a-1989. For ATM and ATM2 IQ2 and IQ2-E interfaces, M23 framing is used when the no-cbit-parity statement is included. For all other interfaces, M13 framing is used when the no-cbit-parity statement is included.

Default  C-bit parity mode is enabled.

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

Related Documentation  • Configuring E3 and T3 Parameters on ATM Interfaces
                      • Disabling T3 C-Bit Parity Mode
core-dump

Syntax  (core-dump | no-core-dump);

Hierarchy Level  [edit interfaces mo-fpc/pic/port multiservice-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For monitoring services interfaces only, a useful tool for isolating the cause of a problem. Core dumping is enabled by default. The directory /var/tmp contains core files. The Junos OS saves the current core file (0) and the four previous core files, which are numbered 1 through 4 (from newest to oldest):

- core-dump—Enable the core dumping operation.
- no-core-dump—Disable the core dumping operation.

Required Privilege Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring Multiservice Physical Interface Properties on page 154
  • Junos OS Services Interfaces Library for Routing Devices
**feac-loop-respond**

**Syntax**  
(feac-loop-respond | no-feac-loop-respond);

**Hierarchy Level**  
[edit interfaces interface-name t3-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For T3 interfaces only, configure the router so a remote CSU can place the local router into loopback.

If you configure remote or local loopback with the T3 loopback statement, the router does not respond to FEAC requests from the CSU even if you include the feac-loop-respond statement in the configuration. For the router to respond, you must delete the loopback statement from the configuration.

You must rollback the setting done on the remote CSU prior to deactivating the feac-loop-respond statement. If the remote CSU cannot comply, clear the remote loop through local configuration to achieve the cleanup. For example, configure remote loopback on the interface and then delete the remote loopback.

**Default**  
The router does not respond to FEAC requests.

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

**Related Documentation**  
- Configuring the T3 FEAC Response
- loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3) on page 760
- remote-loopback-respond on page 955
flow-control

Syntax  
(flow-control | no-flow-control);

Hierarchy Level  
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options],
[edit interfaces interface-name multiservice-options],
[edit interfaces interface-range name aggregated-ether-options],
[edit interfaces interface-range name ether-options]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 in EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description  
For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the router or switch to the remote side of the connection. Enabling flow control is useful when the remote device is a Gigabit Ethernet switch. Flow control is not supported on the 4-port Fast Ethernet PIC.

NOTE: On the Type 5 FPC, to prioritize control packets in case of ingress oversubscription, you must ensure that the neighboring peers support MAC flow control. If the peers do not support MAC flow control, then you must disable flow control.

Default  
Flow control is enabled.

NOTE: Flow control is enabled by default only on physical interfaces and it is disabled by default on aggregated Ethernet interfaces.

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

Related Documentation  
- Configuring Flow Control
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support
gratuitous-arp-reply

Syntax  (gratuitous-arp-reply | no-gratuitous-arp-reply);

Hierarchy Level  [edit interfaces interface-name]
                  [edit interfaces interface-range interface-range-name]

Release Information  Statement introduced before Junos OS Release 7.4.
                       Statement introduced in Junos OS Release 9.0 in EX Series switches.
                       Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description  For Ethernet interfaces, enable updating of the Address Resolution Protocol (ARP) cache for gratuitous ARPs.

Default  Updating of the ARP cache is disabled on all Ethernet interfaces.

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

Related Documentation  • Configuring Gratuitous ARP
                       • no-gratuitous-arp-request on page 831
no-gratuitous-arp-request

**Syntax**  
no-gratuitous-arp-request;

**Hierarchy Level**  
[edit interfaces interface-name]

**Release Information**  
Statement introduced in Junos OS Release 9.6 for EX Series switches.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

**Description**  
For Ethernet interfaces and pseudowire logical interfaces, do not respond to gratuitous ARP requests.

**Default**  
Gratuitous ARP responses are enabled on all Ethernet interfaces.

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

**Related Documentation**  
• Configuring Gratuitous ARP
no-keepalives

Syntax  no-keepalives;

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

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Disable the sending of keepalives on a physical interface configured with PPP, Frame Relay, or Cisco HDLC encapsulation. The default keepalive interval is 10 seconds.

For ATM2 IQ interfaces only, you can disable keepalives on a logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- `atm-ppp-llc`—PPP over AAL5 LLC encapsulation.
- `atm-ppp-vc-mux`—PPP over AAL5 multiplex encapsulation.

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

Related Documentation  • Configuring Keepalives on page 118
                       • Disabling the Sending of PPPoE Keepalive Messages
                       • Configuring Frame Relay Keepalives
long-buildout

**Syntax**

(long-buildout | no-long-buildout);

**Hierarchy Level**

[edit interfaces interface-name t3-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure the T3 line buildout. A T3 interface has two settings for the T3 line buildout: a short setting, which is less than 255 feet (68 meters), and a long setting, which is greater than 255 feet and shorter than 450 feet (137 meters).

This statement applies to copper-cable-based T3 interfaces only. You cannot configure a line buildout for a DS3 channel on a channelized OC12 interface, which runs over fiber-optic cable.

**Default**

A T3 interface uses the short line buildout setting (no-long-buildout) for wires shorter than 255 feet (68 meters).

**Required Privilege Level**

interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

**Related Documentation**

- Configuring the T3 Line Buildout
loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet)

Syntax  
(loopback | no-loopback);

Hierarchy Level  
[edit interfaces interface-name aggregated-ether-options],  
[edit interfaces interface-name ether-options],  
[edit interfaces interface-name fastether-options],  
[edit interfaces interface-name gigether-options],  
[edit interfaces interface-range name ether-options]

For QFX Series and EX Series:

[edit interfaces interface-name aggregated-ether-options],  
[edit interfaces interface-name ether-options],

For SRX Series Devices and vSRX:

[edit interfaces interface-name redundant-ether-options]

Release Information  
Statement introduced before Junos OS Release 7.4 for MX Series.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.  
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.  
Statement modified in Junos OS Release 9.2 for the SRX Series.

Description  
For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, enable or disable loopback mode.

NOTE:

- By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system.
- IPv6 Neighbor Discovery Protocol (NDP) addresses are not supported on Gigabit Ethernet interfaces when loopback mode is enabled on the interface. That is, if the loopback statement is configured at the [edit interfaces ge-fpc/pic/port gigether-options] hierarchy level, an NDP address cannot be configured at the [edit interfaces ge-fpc/pic/port unit logical-unit-number family inet6 address] hierarchy level.

Default  
By default, loopback is disabled.
mac-learn-enable

Syntax  
mac-learn-enable;

Hierarchy Level  
[edit interfaces interface-name gigether-options ethernet-switch-profile]  
[edit interfaces aex aggregated-ether-options ethernet-switch-profile]

Release Information  
Statement introduced before Junos OS Release 7.4.  

Description  
For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), for Gigabit Ethernet DPCs on MX Series routers, for 100-Gigabit Ethernet Type 5 PIC with CFP, and for MPC3E, MPC4E, MPC5E, MPC5EQ, and MPC6E MPCs, configure dynamic learning of the source and destination MAC addresses. By default, the interface is not allowed to dynamically learn source and destination MAC addresses.

To disable dynamic learning of the source and destination MAC addresses after it has been configured, you must delete mac-learn-enable from the configuration.

MPCs support MAC address accounting for an individual interface or an aggregated Ethernet interface member link only after the interface has received traffic from the MAC source. If traffic is only exiting an interface, the MAC address is not learned and MAC address accounting does not occur.

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

Related Documentation  
• Configuring MAC Address Filtering  
• Configuring MAC Address Accounting
no-partition

Syntax  
no-partition interface-type (e1 | (cau4 | so) | (ct3 | t3) | so | t3);

Hierarchy Level  
[edit interfaces cel-fpc/pic/port],
[edit interfaces coc1-fpc/pic/port:channel],
[edit interfaces coc12-fpc/pic/port],
[edit interfaces cstm1-fpc/pic/port],
[edit interfaces ct3-fpc/pic/port]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For Channelized E1 IQ PICs only, configure the channelized E1 interface as an unpartitioned, clear channel.

For Channelized OC12 PIC only, convert the channelized OC12 IQ interface into a channelized T3 interface or a T3 interface. You perform this configuration task for C-bit parity and M13-mapped configurations.

For Channelized OC12 IQ PICs only, configure the channelized OC12 interface as an unpartitioned, clear channel.

For Channelized STM1 PIC only, convert the channelized STM1 IQ interface into a channelized Administrative Unit 4 (AU-4) interface or a SONET/SDH STM1 interface.

For Channelized DS3 PIC only, configure the channelized T3 interface as an unpartitioned, clear channel.

Default  
If you do not include either this statement or the partition statement, the Channelized IQ PIC is not partitioned, and no data channels are configured.

Options  
The option used must correspond to the physical interface type:

e1—E1 interface type.

coc12 so—Channelized OC12 interface type, in SONET mode.

cau4—Channelized AU-4 interface type.

cstm1—SONET/SDH STM1 interface type, in SDH mode.

ct3—Channelized T3 interface type.

t3—T3 interface type.

Required Privilege Level  
interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.
Related Documentation

- Channelized E1 IQ and IQE Interfaces Overview
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
- Configuring an OC12/STM4 Interface
- Configuring Channelized STM1 IQ and IQE Interfaces
- Configuring T3 IQ Interfaces
- partition on page 871
- no-partition
payload-scrambler

Syntax (payload-scrambler | no-payload-scrambler);

Hierarchy Level [edit interfaces interface-name e3-options], [edit interfaces interface-name sonet-options], [edit interfaces interface-name t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable or disable HDLC scrambling on an E3, a SONET/SDH, or a T3 interface. This type of scrambling provides better link stability. Both sides of a connection must either use or not use scrambling.

If you commit a T3 interface configuration that has HDLC payload scrambling enabled, the interface must also be configured to be compatible with the channel service unit (CSU) at the remote end of the line.

Disable payload scrambling on an E3 interface if Digital Link compatibility mode is used.

On a channelized OC12 interface, the sonet payload-scrambler statement is ignored. To configure scrambling on the DS3 channels on the interface, you can include the t3-options payload-scrambler statement in the configuration for each DS3 channel.

NOTE: The payload-scrambler statement at the [edit interfaces interface-name e3-options] hierarchy level is not valid for IQE PICs.

Default Payload scrambling is disabled on all E3 and T3 interfaces; it is enabled by default on E3/T3 over ATM interfaces and on SONET/SDH interfaces.

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

Related Documentation • Configuring E3 and T3 Parameters on ATM Interfaces
• Configuring E3 HDLC Payload Scrambling
• Configuring SONET/SDH HDLC Payload Scrambling for Link Stability
• Configuring T3 HDLC Payload Scrambling
• Examples: Configuring T3 Interfaces
• compatibility-mode on page 477
## no-pre-classifier

### Syntax

```plaintext
no-pre-classifier;
```

### Hierarchy Level

```
[edit chassis fpc n pic n]
```

### Release Information

Statement introduced in Junos OS Release 10.4.

### Description

Specify disabling the control queue for all ports on the 10-Gigabit Ethernet LAN/WAN PIC. Deleting this configuration re-enables the control queue feature on all ports of the 10-Gigabit Ethernet LAN/WAN PIC.

### NOTE:

For the 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (model number PD-5-10XGE-SFPP), the control queue has a rate limiter to limit the control traffic to 2 Mbps (fixed, not user-configurable) per port. If the transit control traffic crosses this limit, then it can cause drops on locally terminating control traffic, causing flap of protocols such as BGP and OSPF. To avoid the control traffic being dropped, configure the `no-pre-classifier` statement to disable the control queue.

### Default

The `no-pre-classifier` statement is not configured and the control queue is operational.

### Required Privilege Level

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

### Related Documentation

- [10-port 10-Gigabit Ethernet LAN/WAN PIC Overview](#)
- [Disabling Control Queue Disable on a 10-port 10-Gigabit Ethernet LAN/WAN PIC](#)
no-redirects

Syntax  no-redirects;

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

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

Description  Do not send protocol redirect messages on the interface.
  To disable the sending of protocol redirect messages for the entire router or switch,
  include the no-redirects statement at the [edit system] hierarchy level.

Default  Interfaces send protocol redirect messages.

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

Related Documentation  • Disabling the Transmission of Redirect Messages on an Interface on page 210
  • Junos OS Administration Library
source-filtering

Syntax  (source-filtering | no-source-filtering):

Hierarchy Level  [edit interfaces interface-name aggregated-ether-options],
                [edit interfaces interface-name fastether-options],
                [edit interfaces interface-name gigether-options]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.

Description  For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and Gigabit Ethernet IQ interfaces only, enable the filtering of MAC source addresses, which blocks all incoming packets to that interface. To allow the interface to receive packets from specific MAC addresses, include the source-address-filter statement.

If the remote Ethernet card is changed, the interface is no longer able to receive packets from the new card because it has a different MAC address.

Default  Source address filtering is disabled.

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

Related Documentation  • Configuring MAC Address Filtering for Ethernet Interfaces
• Configuring MAC Address Filtering on PTX Series Packet Transport Routers
• accept-source-mac on page 391
• source-address-filter on page 1005
**syslog (Monitoring)**

**Syntax**
(syslog | no-syslog);

**Hierarchy Level**
[edit interfaces mo-fpc/pic/port multiservice-options]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
System logging is enabled by default. The system log information of the Monitoring Services PIC is passed to the kernel for logging in the /var/log directory.

- **syslog**—Enable PIC system logging.
- **no-syslog**—Disable PIC system logging.

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

**Related Documentation**
- Configuring Multiservice Physical Interface Properties on page 154
- Junos OS Services Interfaces Library for Routing Devices
no-termination-request

Syntax  no-termination-request;

Hierarchy Level  [edit interfaces interface-name ppp-options],
[edit interfaces lsq-fpc/pic/port lsq-failure-options]

Release Information  Statement introduced in Junos OS Release 7.4.
Support at the [edit interfaces interface-name ppp-options] hierarchy level added in Junos OS Release 8.3.

Description  For LSQ PICs or link PICs in redundant LSQ configurations, you can inhibit the router from sending PPP termination-request messages to the remote host if the PIC fails.

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

Related Documentation  • Configuring Link PIC Failover on Channelized OC3 IQ and IQE Interfaces
• Configuring Link PIC Failover on Channelized OC12/STM4 IQ and IQE Interfaces
• Configuring Link PIC Failover on Channelized STM1 Interfaces
• Junos OS Services Interfaces Library for Routing Devices
translate-discard-eligible

Syntax  
(translate-discard-eligible | no-translate-discard-eligible);

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

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay discard eligible (DE) control bits.

Default  
DE bit translation is disabled.

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

Related Documentation  
• Configuring Frame Relay Control Bit Translation

translate-fecn-and-becn

Syntax  
(translate-fecn-and-becn | no-translate-fecn-and-becn);

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

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay forward explicit congestion notification (FECN) control bits and Frame Relay backward explicit congestion notification (BECN) control bits.

Default  
FECN and BECN bit translation is disabled.

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

Related Documentation  
• Configuring Frame Relay Control Bit Translation
unframed

Syntax  (unframed | no-unframed);

Hierarchy Level  [edit interfaces interface-name e3-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For E3 IQ interfaces only, enable or disable unframed mode. In unframed mode, the E3 IQ interface do not detect yellow (ylw) or loss-of-frame (lof) alarms.

Default  Unframed mode is disabled.

Required Privilege
Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring E3 IQ and IQE Unframed Mode

z0-increment

Syntax  (z0-increment | no-z0-increment);

Hierarchy Level  [edit interfaces interface-name sonet-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure an incremental STM ID rather than a static one.

Default  no-Z0-increment

Required Privilege
Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode

• sonet-options on page 1002
node-id

Syntax  node-id mac-address;

Hierarchy Level  [edit protocols protection-group ethernet-ring ring-name]


Description  For EX Series switches and QFX Series switches, node-id is not configurable.
For MX Series routers, optionally specify the MAC address of a node in the protection group. If this statement is not included, the router assigns the node's MAC address.

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

Related Documentation  • Ethernet Ring Protection Switching Overview
  • Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
  • Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS

non-revertive (Interfaces)

Syntax  non-revertive;

Hierarchy Level  [edit interfaces aeX aggregated-ether-options lACP link-protection]

Release Information  Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.4 for EX Series switches.
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

Description  Disable the ability to switch to a better priority link (if one is available) once a link is established as active and collection distribution is enabled.

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

Related Documentation  • link-protection on page 741
  • Configuring Aggregated Ethernet Link Protection
  • Configuring LACP Link Protection of Aggregated Ethernet Interfaces for Switches
oam

Syntax  oam {
  ethernet {
    connectivity-fault-management {
      action-profile profile-name {
        default-actions {
          interface-down;
        }
      }
    }
    performance-monitoring {
      delegate-server-processing;
      hardware-assisted-timestamping;
      hardware-assisted-keepalives;
      sla-iterator-profiles {
        profile-name {
          avg-fd-twoway-threshold;
          avg-ifdv-twoway-threshold;
          avg-fir-forward-threshold;
          avg-fir-backward-threshold;
          disable;
          calculation-weight {
            delay delay-weight;
            delay-variation delay-variation-weight;
          }
          cycle-time milliseconds;
          iteration-period connections;
          measurement-type (loss | statistical-frame-loss | two-way-delay);
        }
      }
    }
  }
  linktrace {
    age (30m | 10m | 1m | 30s | 10s);
    path-database-size path-database-size;
  }
  maintenance-domain domain-name {
    level number;
    name-format (character-string | none | dns | mac+2octet);
    maintenance-association ma-name {
      short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
      protect-maintenance-association protect-ma-name;
      remote-maintenance-association remote-ma-name;
      continuity-check {
        convey-loss-threshold;
        hold-interval minutes;
        interface-status-tlv;
        interval (100ms | 10m | 10ms | 10s | 1m | 1s);
        loss-threshold number;
        port-status-tlv;
      }
      mep mep-id {
        auto-discovery;
        direction (up | down);
      }
    }
  }
}
interface interface-name (protect | working);
lowest-priority-defect (all-defects | err-xcon | mac-rem-err-xcon | no-defect | rem-err-xcon | xcon);
priority number;
remote-mep mep-id {
  action-profile profile-name;
  sla-iterator-profile profile-name {
    data-tlv-size size;
    iteration-count count-value;
    priority priority-value;
  }
}
}
}
}
link-fault-management {
  action-profile profile-name {
    action {
      link-down;
      send-critical-event;
      syslog;
    }
    event {
      link-adjacency-loss;
      link-event-rate {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
      }
      protocol-down;
    }
  }
}
interface interface-name {
  apply-action-profile
  link-discovery (active | passive);
  loopback-tracking;
  pdu-interval interval;
  pdu-threshold threshold-value;
  remote-loopback;
  event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
  }
  negotiation-options {
    allow-remote-loopback;
    no-allow-link-events;
  }
}
}
<table>
<thead>
<tr>
<th>Hierarchy Level</th>
<th>[edit protocols]</th>
</tr>
</thead>
</table>
| Release Information | Statement introduced in Junos OS Release 8.2.  
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers. |
| Description      | For Ethernet interfaces on M320, M120, MX Series, and T Series routers and PTX Series Packet Transport Routers, provide IEEE 802.3ah Operation, Administration, and Maintenance (OAM) support.  
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 | • IEEE 802.3ah OAM Link-Fault Management Overview |
**oam-liveness**

**Syntax**

```plaintext
doam-liveness {
down-count cells;
up-count cells;
}
```

**Hierarchy Level**

- `edit interfaces interface-name atm-options vpi vpi-identifier`,
- `edit interfaces interface-name unit logical-unit-number`,
- `edit interfaces interface-name unit logical-unit-number family family address address` multipoint-destination `address`,
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number`,
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address multipoint-destination address`

**Release Information**

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

**Description**

For ATM encapsulation only, configure Operation, Administration, and Maintenance (OAM) F5 loopback cell count thresholds. Not supported on ATM-over-SHDSL interfaces.

For ATM2 IQ PICs only, configure OAM F4 loopback cell count thresholds at the `edit interfaces interface-name atm-options vpi vpi-identifier` hierarchy level.

**Options**

- **down-count cells**—Minimum number of consecutive OAM F4 or F5 loopback cells lost before a VC is declared down.
  - **Range:** 1 through 255
  - **Default:** 5 cells

- **up-count cells**—Minimum number of consecutive OAM F4 or F5 loopback cells received before a VC is declared up.
  - **Range:** 1 through 255
  - **Default:** 5 cells

**Required Privilege Level**

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

**Related Documentation**

- Configuring the ATM OAM F5 Loopback Cell Threshold
# oam-period

**Syntax**

```plaintext
oam-period (disable | seconds);
```

**Hierarchy Level**

- `edit interfaces interface-name atm-options vpi vpi-identifier`.
- `edit interfaces interface-name unit logical-unit-number`.
- `edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address`.
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number`.
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address multipoint-destination address`.

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

For ATM encapsulation only, configure the OAM F5 loopback cell period. Not supported on ATM-over-SHDSL interfaces.

For ATM2 IQ PICs only, configure the OAM F4 loopback cell period at the `edit interfaces interface-name atm-options vpi vpi-identifier` hierarchy level.

**Default**

If you omit this statement, OAM F5 loopback cells are not initiated, but the interface still responds if it receives OAM F5 loopback cells.

**Options**

- `disable`—Disable the OAM loopback cell transmit feature.
- `seconds`—OAM loopback cell period.
  
  **Range**: 1 through 900 seconds

**Required Privilege Level**

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

**Related Documentation**

- *Defining the ATM OAM F5 Loopback Cell Period*
**oc-slice**

**Syntax**  
`oc-slice oc-slice-range;`

**Hierarchy Level**  
[edit interfaces interface-name partition partition-number]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For channelized OC12 IQ interfaces only, configure the range of SONET/SDH slices.

**Default**  
If you do not include either this statement or the **no-partition** statement, the Channelized OC12 IQ PICs not partitioned, and no data channels are configured.

**Options**  
`oc-slice-range`—Range of SONET/SDH slices. OC3 interfaces must occupy three consecutive OC slices per interface, in the form 1–3, 4–6, 7–9, or 10–12. The T3, T1, and DS0 interface types each occupy one OC slice per interface.

**Range:**  
For OC3 interfaces, 1–3, 4–6, 7–9, or 10–12; for SONET/SDH and T3 interfaces, 1–12

The remaining statement is 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**  
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
open-timeout

Syntax  open-timeout seconds;

Hierarchy Level  [edit interfaces interface-name services-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure timeout period for Transmission Control Protocol (TCP) session establishment.

Options  seconds—Timeout period in seconds.
  Range: 4 through 224 seconds
  Default: 5 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 Services Interfaces Library for Routing Devices
operating-mode

Syntax  
operating-mode mode;

Hierarchy Level  
[edit interfaces at-fpc/pic/port dsl-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For J Series Services Routers only, modify the operating mode of the digital subscriber line for an ATM interface.

Options  

mode—Operating mode for ATM-over-ADSL interfaces. The mode can be one of the following:

- adsl2plus—Set the ADSL line to train in the ITU G.992.5 mode.
- ansi-dmt—Set the ADSL line to train in the ANSI T1.413 Issue 2 mode.
- auto—Set the ADSL line to autonegotiate the setting to match the setting of the DSL access multiplexer (DSLAM) located at the central office. The ADSL line trains in the ANSI T1.413 Issue 2 (ansi-dmt) or ITU G.992.1 (itu-dmt) mode.
- etsi—Set the ADSL line to train in the ETSI TS 101 388 V1.3.1 mode.
- itu-annexb-ur2—Set the ADSL line to train in the ITU G.992.1 UR-2 mode.
- itu-annexb-non-ur2—Set the ADSL line to train in the ITU G.992.1 non-UR-2 mode.
- itu-dmt—Set the ADSL line to train in the ITU G.992.1 mode.
- itu-dmt-bis—Set the ADSL line to train in the ITU G.992.3 mode.

Default: auto

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

Related Documentation  
- ATM-over-ADSL Overview
- Junos OS Interfaces and Routing Configuration Guide
## optics-options

**Syntax**

```plaintext
options-options {
  alarm low-light-alarm {
    (link-down | syslog);
  }
  tca tca-identifier (enable-tca | no-enable-tca) (threshold number | threshold-24hrs number); tx-power dbm;
  warning low-light-warning {
    (link-down | syslog);
  }
  wavelength nm;
  loopback;
}
```

**Hierarchy Level**

```
[edit interfaces interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
- **alarm** option and **warning** options introduced in Junos OS Release 10.0.
- Statement introduced in Junos OS Release 12.1 for EX Series switches.
- Statement and **tx-power** option introduced in Junos OS Release 13.2 for PTX Series routers.
- **tca** option introduced in Junos OS Release 14.2 for PTX Series routers.
- Statement introduced in Junos OS Release 18.3R1 for PTX10K-LC1104 on the PTX10008 and PTX10016 routers.
- Statement introduced in Junos OS Release 18.3R1 for ACX6360 routers.
- **loopback** option introduced in Junos OS Release 19.2R1 for QSFP-100GE-DWDM2 transceiver on MX10003, MX10008, MX10016, and MX204 routers.

**Description**

For 10-Gigabit Ethernet or 100-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces only, configure full C-band International Telecommunication Union (ITU)-Grid tunable optics.

On the PTX Series routers, when an interface is configured in 8QAM mode, you must configure both the optics from a AC400 module with the same optics-options for the links to come up.

**Options**

- **loopback**—Displays the electrical loopback status of QSFP-100GE-DWDM2 transceiver on MX10003, MX10008, MX10016, and MX204 routers.

  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.
option-82

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

```
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Options `circuit-id` and `remote-id` introduced in Junos OS Release 11.4.

Description

Specify that the option 82 information from the client PDU is concatenated with the username during the subscriber authentication process.

For autosense VLANs, you can additionally specify Option 82 suboption information that is concatenated with the username. You can specify either both or neither of the Agent Circuit ID (suboption 1) and Agent Remote ID (suboption 1). 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.

NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the incoming DHCP discover packet. The use of suboptions is supported for DHCPv4 only.

Options

- **none**—Use the raw payload of Option 82 from the PDU.
- **circuit-id**—(Optional) Use the Agent Circuit ID suboption (suboption 1).
- **remote-id**—(Optional) Use 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

- Configuring VLAN Interface Username Information for AAA Authentication
- Using DHCP Option 82 Suboptions in Authentication Usernames for Autosense VLANs
otn-options

Syntax

```
otn-options {
  bytes (otn-options) transmit-payload-type value;
  fec (efec | gfec | gfec-sdfec | none);
  (is-ma | no-is-ma);
  (laser-enable | no-laser-enable);
  (line-loopback | no-line-loopback);
  (local-loopback | no-local-loopback);
  (odu-ttim-action-enable | no-odu-ttim-action-enable);
  (otu-ttim-action-enable | no-otu-ttim-action-enable);
  odu-delay-management {
    (bypass | no-bypass);
    (monitor-end-point | no-monitor-end-point);
    number-of-frames value;
    (no-start-measurement | start-measurement;
  }
  odu-signal-degrade {
    ber-threshold-clear value;
    ber-threshold-signal-degrade value;
    interval value;
  }
  (prbs | no-prbs);
  preemptive-fast-reroute {
    (backward-frr-enable | no-backward-frr-enable);
    (signal-degrade-monitor-enable | no-signal-degrade-monitor-enable);
    odu-backward-frr-enable | no-odu-backward-frr-enable;
    odu-signal-degrade-monitor-enable | no-odu-signal-degrade-monitor-enable;
  }
  rate {
    (fixed-stuff-bytes | no-fixed-stuff-bytes);
    oc192;
    otu4;
    (pass-through | no-pass-through);
  }
  signal-degrade {
    ber-threshold-clear value;
    ber-threshold-signal-degrade value;
    interval value;
  }
  tca tca-identifier (enable-tca | no-enable-tca) (threshold number | threshold-24hrs number);
  transport-monitoring;
  trigger trigger-identifier;
  tti tti-identifier;
}
```

Hierarchy Level

- [edit interfaces ge-fpc/pic/port]
- [edit interfaces xe-fpc/pic/port]
- [edit interfaces et-fpc/pic/port]

Release Information

Statement introduced in Junos OS Release 9.4.
<table>
<thead>
<tr>
<th>Description</th>
<th>Specify the Ethernet optical transport network (OTN) interface and options.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>The remaining statements are explained separately. See CLI Explorer.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>interfaces—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>interfaces-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- 10-Gigabit Ethernet OTN Options Configuration Overview
- 100-Gigabit Ethernet OTN Options Configuration Overview
- Configuring OTN Interfaces on P1-PTX-2-100G-WDM


**oc192** statement introduced in Junos OS Release 13.3R3 for MX Series routers.


tca option introduced in Junos OS Release 14.2 for PTX Series routers.

bytes, line-loopback, local-loopback, preemptive-fast-reroute, tca, trigger, prbs, and tti statements introduced in 18.3R1 for ACX6360 routers.
output

Syntax

```
output {
    service-set service-set-name <service-filter filter-name>;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet service],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet service]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more output service sets and filters to be applied to traffic.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Junos OS Services Interfaces Library for Routing Devices
output-list

Syntax

```
output-list [ filter-names ];
```

Hierarchy Level

- [edit interfaces interface-name unit logical-unit-number family family filter],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family filter]

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Apply a group of filters to evaluate when packets are transmitted on an interface.

Options

**[ filter-names ]**—Name of a filter to evaluate when packets are transmitted on the interface. Up to 16 filters can be included in a filter input list.

Required Privilege

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

Related Documentation

- Applying a Filter to an Interface on page 220
- input-list on page 680
- Routing Policies, Firewall Filters, and Traffic Policers Feature Guide
- Junos OS Services Interfaces Library for Routing Devices
- Junos OS Administration Library
output-policer

Syntax  output-policer policer-name;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number layer2-policer],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number layer2-policer]

Release Information  Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Apply a single-rate two-color policer to the Layer 2 output traffic at the logical interface. The output-policer and output-three-color statements are mutually exclusive.

Options  policer-name—Name of the single-rate two-color policer that you define at the [edit firewall] hierarchy level.

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

Related Documentation  • Two-Color and Three-Color Policers at Layer 2
• Applying Layer 2 Policers to Gigabit Ethernet Interfaces
• Configuring a Gigabit Ethernet Policier
• input-policer on page 681
• input-three-color on page 683
• layer2-policer on page 726
• logical-interface-policer on page 755
• output-three-color on page 863
### output-priority-map

**Syntax**

```plaintext
classifier {
  premium {
    forwarding-class class-name {
      loss-priority (high | low);
    }
  }
}
```

**Hierarchy Level**

- [edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]
- [edit interfaces interface-name ether-options ethernet-switch-profile ethernet-policer-profile]

**Release Information**

Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 13.2 for the QFX Series.

**Description**

For Gigabit Ethernet IQ and 10-Gigabit Ethernet interfaces only, define the output policer priority map to be applied to outgoing frames on this interface.

The remaining statements are explained separately. See [CLI Explorer](#).

**Required Privilege**

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

**Related Documentation**

- [Specifying an Output Priority Map](#)
- input-priority-map on page 682
### output-three-color

**Syntax**

```
output-three-color policer-name;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number layer2-policer]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number layer2-policer]
```

**Release Information**

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Apply a single-rate or two-rate three-color policer to the Layer 2 output traffic at the logical interface. The `output-three-color` and `output-policer` statements are mutually exclusive.

**Options**

- **policer-name**—Name of the single-rate or two-rate three-color policer.

**Required Privilege Level**

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

**Related Documentation**

- Two-Color and Three-Color Policers at Layer 2
- Applying Layer 2 Policers to Gigabit Ethernet Interfaces
  - Configuring a Gigabit Ethernet Policer
- `input-three-color` on page 683
- `input-policer` on page 681
- `layer2-policer` on page 726
- `logical-interface-policer` on page 755
- `output-policer` on page 861
output-vlan-map (Aggregated Ethernet)

**Syntax**

```output-vlan-map {
  (pop | push | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
```

**Hierarchy Level**

- [edit interfaces interface-name unit logical-unit-number],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced in Junos OS Release 8.2.
Starting in Junos OS Release 17.3R1, input-vlan-map for outer vlan is supported for L2 circuit over aggregated Ethernet interfaces for QFX10000 Series switches.

**Description**

Define the rewrite profile to be applied to outgoing frames on this logical interface. On MX Series routers, this statement only applies to aggregated Ethernet interfaces using Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ2 and IQ2-E interfaces and 100-Gigabit Ethernet Type 5 PIC with CFP.

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**

- Stacking and Rewriting Gigabit Ethernet VLAN Tags
- input-vlan-map (Aggregated Ethernet) on page 684
**output-vlan-map**

Syntax

```plaintext
output-vlan-map {
   (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
   inner-tag-protocol-id tpid;
   inner-vlan-id number;
   tag-protocol-id tpid;
   vlan-id number;
}
```

Hierarchy Level

```plaintext
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

For EX Series switches, defines the rewrite operation to be applied to outgoing frames.

For MX Series routers and NFX Series devices' Gigabit Ethernet IQ and 10-Port 10-Gigabit Ethernet SFPP interfaces only, defines the rewrite operation to be applied to outgoing frames on this logical interface.

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

- Stacking and Rewriting Gigabit Ethernet VLAN Tags
- input-vlan-map on page 685
overflow (Receive Bucket)

Syntax  
overflow (discard | tag);

Hierarchy Level  
[edit interfaces interface-name receive-bucket]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Specify how to handle packets that exceed the threshold for the receive leaky bucket.

Options  
tag—Tag, count, and process received packets that exceed the threshold.

discard—Discard received packets that exceed the threshold. No counting is done.

Required Privilege  

Level  
interface—To view this statement in the configuration.

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

Related Documentation  
• Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140

overflow (Transmit Bucket)

Syntax  
overflow discard;

Hierarchy Level  
[edit interfaces interface-name transmit-bucket]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
Discard packets that exceed the threshold for the transmit leaky bucket.

Required Privilege  

Level  
interface—To view this statement in the configuration.

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

Related Documentation  
• Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140
override

Syntax:  
```
override tag vlan-tag dynamic-profile profile name;
```

Hierarchy Level:  
```
[edit interfaces interface-name auto-configure vlan-ranges],
[edit interfaces interface-name auto-configure stacked-vlan-ranges]
```

Release Information:  
Statement introduced in Junos OS Release 11.2.

Description:  
Override dynamic profile assignment to individual VLANs that are already part of a previously defined VLAN range and dynamic profile.

Options:  
- `vlan-tag`—VLAN tag that you want to override.
- `profile-name`—Name of the dynamic profile that you want to use when overriding the specified VLAN tag.

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

Related Documentation:  
- [Overriding the Dynamic Profile Used for an Individual VLAN](#)
- [Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs](#)
- [Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs](#)
**pado-advertise**

**Syntax**

```
pado-advertise;
```

**Hierarchy Level**

```
[edit protocols pppoe]
```

**Release Information**

Statement introduced in Junos OS Release 10.2.

**Description**

Enable named services configured in PPPoE service name tables to be advertised in PPPoE Active Discovery Offer (PADO) control packets. By default, advertisement of named services in PADO packets is disabled.

**NOTE:** If you enable advertisement of named services in PADO packets, make sure the number and length of all advertised service entries does not exceed the maximum transmission unit (MTU) size of the PPPoE underlying interface.

**Required Privilege**

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

**Related Documentation**

- Configuring PPPoE Service Name Tables
- Enabling Advertisement of Named Services in PADO Control Packets
paired-group

**Syntax**  
paired-group *group-name*;

**Hierarchy Level**  
[edit interfaces *interface-name* sonet-options *aps*]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
Configure load sharing between two working protect circuit pairs.

**Options**  
*group-name*—Circuit’s group name, as configured with the *protect-circuit* or *working-circuit* statement.

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

**Related Documentation**  
- Configuring APS Load Sharing  
- working-circuit on page 1148
pap

Syntax

```pap
{access-profile name;
default-pap-password password;
local-name name;
local-password password;
passive; }
```

Hierarchy Level

- [edit interfaces interface-name ppp-options],
- [edit interfaces interface-name unit logical-unit-number ppp-options],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options]

Release Information

Statement introduced in Junos OS Release 8.3.

Description

Configure the Password Authentication Protocol (PAP). Use PAP authentication as a means to provide a simple method for the peer to establish its identity using a two-way handshake. This is done only upon initial link establishment.

After the link is established, an ID and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

**BEST PRACTICE:** On inline service (si) interfaces for L2TP, only the `pap` statement itself is typically used for subscriber management. We recommend that you leave the subordinate statements at their default values.

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

- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
- Configuring the PPP Password Authentication Protocol On a Logical Interface on page 180
- Tracing Operations of the pppd Process on page 137
- traceoptions (PPP Process) on page 1069
- Example: Configuring PAP for an L2TP Profile
- Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface
**partition**

**Syntax**

```
partition partition-number oc-slice oc-slice-range interface-type type timeslots
time-slot-range;
```

**Hierarchy Level**

[edit interfaces interface-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

The partition number is correlated with the channel number. Partition and channel numbering on IQ interfaces begins with :1, not :0.

**Default**

If you omit this statement, the channelized PIC or PIM is not partitioned, and no data channels are configured.

**Options**

- **partition-number**—Sublevel interface partition index.
  - Range:
    - 1 through 4 for an OC3 interface on a channelized OC12 IQ interface.
    - 1 through 12 for a T3 interface on a channelized OC12 IQ interface.
    - 1 through 4 for a T3 interface on a channelized T3 IQ interface.
    - 1 through 28 for a T1 IQ interface on a channelized OC12 IQ or channelized T3 IQ interface.
    - 1 through 10 for an E1 interface on a channelized E1 IQ interface.
    - 1 through 30 on a channelized E1 interface.
    - 1 through 23 on a channelized T1 interface.
    - 1 through 24 for NxDS0 interfaces on either channelized OC12 IQ or channelized DS3 IQ interfaces.
    - 0 through 31 (with 0 reserved for framing) for NxDS0 interfaces on channelized E1 IQ interfaces.

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**

- Channelized E1 IQ and IQE Interfaces Overview
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
- Configuring Channelized T3 IQ Interfaces
- no-partition on page 836
## passive (CHAP)

**Syntax**
```
passive;
```

**Hierarchy Level**
```
[edit interfaces interface-name ppp-options chap],
[edit interfaces interface-name unit logical-unit-number ppp-options chap],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options chap]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Do not challenge the peer, but respond if challenged. If you omit this statement from the configuration, the interface always challenges its peer.

For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- **atm-ppp-llc**—PPP over AAL5 LLC encapsulation.
- **atm-ppp-vc-mux**—PPP over AAL5 multiplex encapsulation.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**
- *Configuring Passive Mode*
passive (PAP)

Syntax

```
passive;
```

Hierarchy Level

```
[edit interfaces interface-name ppp-options pap],
[edit interfaces interface-name unit logical-unit-number ppp-options pap],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options pap]
```

Release Information

Statement introduced in Junos OS Release 8.3.

Description

Initiate an authentication request when the PAP option is received from a peer. If you omit this statement from the configuration, the interface requires the peer to initiate an authentication request.

Required Privilege

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

Related Documentation

- Configuring Passive Mode
- Junos OS Administration Library
passive-monitor-mode

Syntax

```
passive-monitor-mode;
```

Hierarchy Level

```
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Monitor packet flows from another router. If you include this statement in the configuration, the interface does not send keepalives or alarms, and does not participate actively on the network.

This statement is supported on ATM, Ethernet, and SONET/SDH interfaces. For more information, see ATM Interfaces Feature Guide for Routing Devices.

For ATM and Ethernet interfaces, you can include this statement on the physical interface only.

For SONET/SDH interfaces, you can include this statement on the logical interface only.

Required Privilege Level

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

Related Documentation

- Enabling Passive Monitoring on ATM Interfaces
- Passive Monitoring on Ethernet Interfaces Overview
- Enabling Packet Flow Monitoring on SONET/SDH Interfaces
- `multiservice-options on page 808`
- Junos OS Services Interfaces Library for Routing Devices
password (Interfaces)

Syntax  

password password-string;

Hierarchy Level  

[edit interfaces interface-name auto-configure vlan-ranges authentication],  
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication]

Release Information  

Statement introduced in Junos OS Release 10.0.

Description  

Configure the password that is sent to the external AAA authentication server for subscriber VLAN or stacked VLAN interface authentication.

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  

• Configuring an Authentication Password for VLAN or Stacked VLAN Ranges

path-database-size

Syntax  

path-database-size path-database-size;

Hierarchy Level  

[edit protocols oam ethernet connectivity-fault-management linktrace]

Release Information  

Statement introduced in Junos OS Release 8.5.

Description  

Number of linktrace reply entries to be stored per linktrace request.

Options  

path-database-size—Database size.  
Range: 1 through 255  
Default: 64

Required Privilege  

Level  

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

Related Documentation  

• Configuring Linktrace Protocol in CFM
**path-trace**

**Syntax**  
`path-trace trace-string;`

**Hierarchy Level**  
`[edit interfaces interface-name sonet-options]`

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode, configure a path trace identifier, which is a text string that identifies the circuit.

On SONET/SDH OC48 interfaces that are configured for channelized (multiplexed) mode (by including the `no-concatenate` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level), the `bytes e1-quiet` and `bytes f1` options have no effect. The `bytes f2`, `bytes z3`, `bytes z4`, and `path-trace` options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

For DS3 channels on a channelized OC12 interface, you can configure a unique path trace for each of the 12 channels. Each path trace can be up to 16 bytes. For channels on a channelized OC12 IQ interface, each path trace can be up to 64 bytes.

**Options**  
`trace-string`—Text string that identifies the circuit. If the string contains spaces, enclose it in quotation marks. A common convention is to use the circuit identifier as the path trace identifier. If you do not configure an identifier, the Junos OS uses the system and interface names to construct the default `trace-string`. For all nonchannelized SONET/SDH interfaces, the default `trace-string` is `system-name interface-name`. For channelized SONET/SDH interfaces and 10–Gigabit Ethernet WAN-PHY interfaces, the default `trace-string` is `interface-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 SONET/SDH Path Trace Identifier for a Circuit
- `sonet-options` on page 1002
payload-scrambler

Syntax (payload-scrambler | no-payload-scrambler);

Hierarchy Level [edit interfaces interface-name e3-options],
[edit interfaces interface-name sonet-options],
[edit interfaces interface-name t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable or disable HDLC scrambling on an E3, a SONET/SDH, or a T3 interface. This type of scrambling provides better link stability. Both sides of a connection must either use or not use scrambling.

If you commit a T3 interface configuration that has HDLC payload scrambling enabled, the interface must also be configured to be compatible with the channel service unit (CSU) at the remote end of the line.

Disable payload scrambling on an E3 interface if Digital Link compatibility mode is used.

On a channelized OC12 interface, the sonet payload-scrambler statement is ignored. To configure scrambling on the DS3 channels on the interface, you can include the t3-options payload-scrambler statement in the configuration for each DS3 channel.

NOTE: The payload-scrambler statement at the [edit interfaces interface-name e3-options] hierarchy level is not valid for IQE PICs.

Default Payload scrambling is disabled on all E3 and T3 interfaces; it is enabled by default on E3/T3 over ATM interfaces and on SONET/SDH interfaces.

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

Related Documentation • Configuring E3 and T3 Parameters on ATM Interfaces
• Configuring E3 HDLC Payload Scrambling
• Configuring SONET/SDH HDLC Payload Scrambling for Link Stability
• Configuring T3 HDLC Payload Scrambling
• Examples: Configuring T3 Interfaces
• compatibility-mode on page 477
payload-size

Syntax  payload-size bytes ;

Hierarchy Level  [edit interfaces interface-name satop-options]

Release Information  Statement introduced in Junos OS Release 9.3.

Description  Specify the satop-options payload size in integer number of bytes.

Required Privilege Level  

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

Related Documentation  

•  ATM Support on Circuit Emulation PICs Overview  
•  satop-options on page 977
**pdu-interval**

**Syntax**  
pdu-interval interval;

**Hierarchy Level**  
[edit protocols oam ethernet link-fault-management interface interface-name]

**Release Information**  
Statement introduced in Junos OS Release 8.2 for MX, M, T, ACX, Series routers, SRX Series firewalls, and EX Series Switches.  
Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**  
For Ethernet interfaces on EX Series switches and M320, M120, MX Series, and T Series routers, specify the periodic OAM PDU sending interval for fault detection. Used for IEEE 802.3ah Operation, Administration, and Management (OAM) support.

**Options**  
*interval*—Periodic OAM PDU sending interval.  
**Range:** For MX, M, T, ACX, Series routers, SRX Series firewalls and EX Series switches – 100 through 1000 milliseconds  
**Default:** For EX Series switches – 1000 milliseconds

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

**Related Documentation**  
- Configuring the OAM PDU Interval  
- Example: Configuring Ethernet OAM Link Fault Management  
- Configuring Ethernet OAM Link Fault Management
pdu-threshold

Syntax  pdu-threshold threshold-value;

Hierarchy Level  [edit protocols oam ethernet link-fault-management interface interface-name]

Statement introduced in Junos OS Release 9.4 for EX Series switches and NFX Series devices.

Description  Configure how many protocol data units (PDUs) are missed before declaring the peer lost in Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.

For Ethernet interfaces on EX Series switches and M320, M120, MX Series, and T Series routers, specify the number of OAM PDUs to miss before an error is logged. Used for IEEE 802.3ah Operation, Administration, and Management (OAM) support.

Options  threshold-value—The number of PDUs missed before declaring the peer lost.
Range:  3 through 10 PDUs
Default:  3 PDUs

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

Related Documentation  • Configuring the OAM PDU Threshold
• Configuring Ethernet OAM Link Fault Management
peer

Syntax
peer a.b.c.d [ 
    interface interface-name;
] 

Hierarchy Level
[edit interfaces interface-name multi-chassis-protection]

Release Information
Statement introduced in Junos OS Release 11.1.

Description
For MX Series routers with multichassis aggregated Ethernet (MC-AE) interfaces, use the multi-chassis-protection statement under the physical interface level to reduce the configuration at the logical interface level. If the interchassis control protocol connection (ICCP) is UP and the interchassis data link (ICL) comes UP, the router configured as standby will bring up the MC-AE interfaces shared with the peer active-active node specified by the peer statement. You must also specify the peer’s physical interface.

Options
  a.b.c.d—Specify the IP address of the peer.

  interface interface-name—Specify the peer’s physical interface: interface
    interface-name-fpc/pic/port

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

Related Documentation
  • Configuring Multichassis Link Aggregation on MX Series Routers
  • Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers and QFX Series Switches
  • Configuring Aggregated Ethernet Link Protection
  • Example: Configuring Aggregated Ethernet Link Protection
  • multi-chassis-protection on page 801
### peer-unit

**Syntax**

peer-unit unit-number;

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure a peer relationship between two logical systems.

**Options**

- **unit-number**—Peering logical system unit number.

**Required Privilege**

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

**Related Documentation**

- [Junos OS Services Interfaces Library for Routing Devices](#)
per-unit-scheduler

Syntax  
per-unit-scheduler;

Hierarchy Level  
[edit interfaces interface-name]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 13.2 on 16x10GE MPC and MPC3E line cards.  
Statement introduced in Junos OS Release 13.3 on MPC4E line cards.  
Statement introduced in Junos OS Release 15.1 on MPC6E line cards.

Description  
For Channelized OC3 IQ, Channelized OC12 IQ, Channelized ST1 IQ, Channelized T3 IQ,  
Channelized E1 IQ, E3 IQ, link services IQ interfaces (lsq-), Gigabit Ethernet IQ, Gigabit  
Ethernet IQ2 and IQ2-E, and 10-, 40-, and 100-Gigabit Ethernet interfaces (including the  
16x10GE MPC), enable the association of scheduler maps with logical interfaces.

CAUTION:  Turning on per-unit scheduling causes the interface to reinitialize,  
which means all logical interfaces (units) on the interface are deleted and recreated.

NOTE:  To enable per-unit scheduling on MX80 and MX104 routers, configure  
the per-unit-scheduler statement at each member physical interface level of  
a particular aggregated Ethernet interface as well as at that aggregated  
Ethernet interface level. On other routing platforms, it is enough if you include  
this statement at the aggregated Ethernet interface level.

NOTE:  Per-unit scheduling is not supported on T1 interfaces configured on  
the Channelized OC12 IQ PIC.

NOTE:  On Gigabit Ethernet IQ2 and IQ2-E PICs without the per-unit-scheduler  
statement, the entire PIC supports 4071 VLANs and the user can configure  
all the VLANs on the same port.  
On Gigabit Ethernet IQ2 and IQ2-E PICs with the per-unit-scheduler statement,  
the entire PIC supports 1024 – 2 * number of ports (1024 minus two times  
the number of ports), because each port is allocated two default schedulers.
When including the **per-unit-scheduler** statement, you must also include the **vlan-tagging** statement or the **flexible-vlan-tagging** statement (to apply scheduling to VLANs) or the **encapsulation frame-relay** statement (to apply scheduling to DLCIs) at the [edit interfaces interface-name] hierarchy level.

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

**Related Documentation**
- Applying Scheduler Maps and Shaping Rate to DLCIs and VLANs
- `vlan-tagging` on page 1131
- `flexible-vlan-tagging` on page 617
- Example: Applying Scheduling and Shaping to VLANs
- Configuring Virtual LAN Queuing and Shaping on PTX Series Routers
performance-monitoring

Syntax

```
performance-monitoring {
  delegate-server-processing;
  hardware-assisted-timestamping;
  hardware-assisted-keepalives;
  sla-iterator-profiles {
    profile-name {
      avg-fd-twoway-threshold;
      avg-ifdv-twoway-threshold;
      avg-flr-forward-threshold;
      avg-flr-backward-threshold;
      disable;
      calculation-weight {
        delay delay-weight;
        delay-variation delay-variation-weight;
      }
      cycle-time milliseconds;
      iteration-period connections;
      measurement-type (loss | statistical-frame-loss | two-way-delay);
    }
  }
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
```

Release Information

Statement introduced in Junos OS Release 9.5.

Description

Specify performance monitoring support for Ethernet frame delay measurement.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

- Configure—To enter configuration mode.
- Control—To modify any configuration.

Related Documentation

- Ethernet Frame Delay Measurements Overview
- Guidelines for Configuring Routers to Support an ETH-DM Session
- Enabling the Hardware-Assisted Timestamping Option
**periodic**

**List of Syntax**  
Syntax (EX Series) on page 886  
Syntax (QFX Series) on page 886

**Syntax (EX Series)**  
periodic interval;

**Syntax (QFX Series)**  
periodic (fast | slow);

**Hierarchy Level (EX Series)**  
[edit interfaces ae x aggregated-ether-options lACP],  
[edit interfaces interface-range name aggregated-ether-options lACP]

**Hierarchy Level (QFX Series)**  
[edit interfaces ae x aggregated-ether-options lACP]

**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.  
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

**Description**  
For aggregated Ethernet interfaces only, configure the interval for periodic transmission of LACP packets.

**Options**  
*interval*—Interval for periodic transmission of LACP packets.

- *fast*—Transmit packets every second.
- *slow*—Transmit packets every 30 seconds.

Default: *fast*

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

**Related Documentation**  
- Configuring LACP for Aggregated Ethernet Interfaces  
- Configuring Aggregated Ethernet LACP (CLI Procedure)  
  - Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch  
- Configuring Aggregated Ethernet LACP (CLI Procedure)  
- Understanding Aggregated Ethernet Interfaces and LACP for Switches  
- Junos OS Network Interfaces Library for Routing Devices
**pfc**

**Syntax**

`pfc;`

**Hierarchy Level**

- `[edit interfaces interface-name ppp-options compression]`
- `[edit interfaces interface-name unit logical-unit-number ppp-options compression]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ppp-options compression]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For interfaces with PPP encapsulation, configure the router to compress the protocol field to one byte.

**Required Privilege Level**

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

**Related Documentation**

- [Configuring the PPP Protocol Field Compression on page 135](#)

---

**pic-type**

**Syntax**

`pic-type (atm1 | atm2);`

**Hierarchy Level**

- `[edit interfaces atm1 | atm2 atm-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM interfaces, configure the type of ATM PIC installed in your router.

**Options**

- `atm1`—ATM1 PIC.
- `atm2`—ATM2 IQ PIC.

**Required Privilege Level**

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

**Related Documentation**

- [Configuring the ATM PIC Type](#)
**plp-to-clp**

**Syntax**

```
plp-to-clp;
```

**Hierarchy Level**

```
[edit interfaces at-fpc/pic/port atm-options],
[edit interfaces at-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces at--fpc/pic/port unit logical-unit-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces only, enable the PLP setting to be copied to the cell-loss priority (CLP) bit.

**Default**

If you omit this statement, the Junos OS does not copy the PLP setting to the CLP bit.

**Required Privilege Level**

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

**Related Documentation**

- Enabling the PLP Setting to Be Copied to the CLP Bit
- Copying the Packet Loss Priority to the CLP Bit on ATM Interfaces
plp1

Syntax  
plp1 cells;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number],  
[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address]

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

Description  
For ATM2 IQ interfaces only, define the EPD threshold on a VC. The EPD threshold is a limit on the number of transmit packets that can be queued. Packets that exceed the limit are discarded. This threshold applies to packets that have a PLP of 1.

Default  
EPD threshold is unregulated.

Options  
- **cells**—Maximum number of cells.  
  Range:  
  - For 1-port and 2-port OC12 interfaces, 1 through 425,984 cells  
  - For 1-port OC48 interfaces, 1 through 425,984 cells  
  - For 2-port OC3, DS3, and E3 interfaces, 1 through 212,992 cells  
  - For 4-port DS3 and E3 interfaces, 1 through 106,496 cells

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

Related Documentation  
- Configuring Two EPD Thresholds per Queue  
- Configuring an ATM Scheduler Map  
- linear-red-profile on page 733
point-to-point

Syntax

point-to-point;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, configure the interface unit as a point-to-point connection. This is the default connection type.

Default

If you omit this statement, the interface unit is configured as a point-to-point connection.

Required Privilege Level

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

Related Documentation

• Configuring a Point-to-Point Connection on page 177
• multipoint on page 806
policer (CFM Firewall)

Syntax

policer cfm-policer {
  if-exceeding {
    bandwidth-limit 8k;
    burst-size-limit 2k;
  }
  then discard;
}

Hierarchy Level  [edit firewall]

Release Information  Statement introduced in Junos OS Release 10.0.

Description  Attach an explicit policer to CFM sessions.

Required Privilege Level

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

Related Documentation

- Configuring Rate Limiting of Ethernet OAM Messages
- policer (CFM Global) on page 892
- policer (CFM Session) on page 893
policer (CFM Global)

Syntax  

```plaintext
policer {
    all cfm-policer-name;
    continuity-check cfm-policer-name;
    other cfm-policer-name;
}
```

Hierarchy Level  

[edit protocols oam ethernet connectivity-fault-management]

Release Information  
Statement introduced in Junos OS Release 10.0.

Description  
Specify a policer at the global level to police the CFM traffic belonging to all sessions.

Options  

- `continuity-check cfm-policer-name`—Police all continuity check packets with the policer specified.
- `other cfm-policer-name`—Police all non-continuity check packets with the policer specified.
- `all cfm-policer-name`—Police all CFM packets with policer specified. If the `all` option is used, then you cannot specify above two options.

Required Privilege Level  

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

Related Documentation  

- Configuring Rate Limiting of Ethernet OAM Messages
- `policer (CFM Session)` on page 893
**policer (CFM Session)**

**Syntax**

```plaintext
policer {
  all cfm-policer-name;
  continuity-check cfm-policer-name;
  other cfm-policer-name;
}
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain name level number maintenance-association name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.

**Description**

Specify a separate policer to rate-limit packets specific to that session.

**Options**

- `continuity-check cfm-policer-name`—Police continuity check packets belonging to this session.
- `other cfm-policer-name`—Police all non-continuity check packets belonging to this session.
- `all cfm-policer-name`—Police all CFM packets belonging to this session. If the `all` option is used, then you cannot specify the above two options.

**Required Privilege**

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

**Related Documentation**

- *Configuring Rate Limiting of Ethernet OAM Messages*
- *policer (CFM Global) on page 892*
**policer (CoS)**

**Syntax**

```
policer cos-policer-name {
    aggregate {
        bandwidth-limit bps;
        burst-size-limit bytes;
    }
    premium {
        bandwidth-limit bps;
        burst-size-limit bytes;
    }
}
```

**Hierarchy Level**

```
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For Gigabit Ethernet IQ, Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and 100-Gigabit Ethernet Type 5 PIC with CFP, define a CoS policer template to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits. The premium policer is not supported on MX Series routers or for Gigabit Ethernet interfaces with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router).

**Options**

- `cos-policer-name`—Name of one policer to specify the premium bandwidth and burst-size limits, and the aggregate bandwidth and burst-size limits.

  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 Gigabit Ethernet Policers
policer (Interface)

Syntax

policer {
  arp policer-template-name;
  input policer-template-name;
  output policer-template-name;
}

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Apply a policer to an interface.

Options

arp policer-template-name—For inet family only, name of one policer to evaluate when ARP packets are received on the interface.

input policer-template-name—Name of one policer to evaluate when packets are received on the interface.

output policer-template-name—Name of one policer to evaluate when packets are transmitted on the interface.

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

Related Documentation
- Applying Policers on page 210
- Configuring Firewall Filters and Policers for VPLS
- Routing Policies, Firewall Filters, and Traffic Policers Feature Guide
- Junos OS Services Interfaces Library for Routing Devices
policer (MAC)

Syntax

```
policer {
   input cos-policer-name;
   output cos-policer-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number accept-source-mac mac-address mac-address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number accept-source-mac mac-address mac-address]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

For Gigabit Ethernet IQ and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and 100-Gigabit Ethernet Type 5 PIC with CFP, configure MAC policing.

NOTE:

On MX Series routers with Gigabit Ethernet or Fast Ethernet PICs, the following considerations apply:

- Interface counters do not count the 7-byte preamble and 1-byte frame delimiter in Ethernet frames.
- In MAC statistics, the frame size includes MAC header and CRC before any VLAN rewrite/imposition rules are applied.
- In traffic statistics, the frame size encompasses the L2 header without CRC after any VLAN rewrite/imposition rule.

Options

**input cos-policer-name**—Name of one policer to specify the premium bandwidth and aggregate bandwidth.

**output cos-policer-name**—Name of one policer to specify the premium bandwidth and aggregate bandwidth.

Required Privilege Level

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

Related Documentation

- Configuring MAC Address Filtering
### policy-statement

**Syntax**

```plaintext
policy-statement policy-name [{
  term term-name [{
    from {
      as-path-unique-count count (equal | orhigher | orlower);
      family family-name;
      match-conditions;
      policy subroutine-policy-name;
      prefix-list prefix-list-name;
      prefix-list-filter prefix-list-name match-type <actions>;
      protocol protocol-name;
      route-filter destination-prefix match-type <actions>;
      source-address-filter source-prefix match-type <actions>;
      tag value;
      traffic-engineering;
    }
    to {
      match-conditions;
      policy subroutine-policy-name;
    }
    then actions;
  }
  then {
    aggregate-bandwidth;
    dynamic-tunnel-attributes dynamic-tunnel-attributes;
    limit-bandwidth limit-bandwidth;
    multipath-resolve multipath-resolve;
    no-entropy-label-capability;
    prefix-segment {
      index index;
      node-segment;
    }
    priority (high | medium | low);
    resolution-map map-name;
  }
}]
```

**Hierarchy Level**

- [edit dynamic-profiles profile-name policy-options],
- [edit logical-systems logical-system-name policy-options],
- [edit policy-options]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
- Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
- **inet-mdt** option introduced in Junos OS Release 10.0R2.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- **route-target** option introduced in Junos OS Release 12.2.
Statement introduced in Junos OS 14.1X53-D20 for the OCX Series.

- **protocol** and **traffic-engineering** options introduced in Junos OS Release 14.2.
- **no-entropy-label-capability** option introduced in Junos OS Release 15.1.
- **priority** and **tag value** options introduced in Junos OS Release 17.1.
- **as-path-unique-count** option introduced in Junos OS Release 17.2R1.
- **prefix-segment** option introduced in Junos OS Release 17.2R1 for MX Series routers, PTX Series routers, QFX5100 switches, and QFX10000 switches.
- **multipath-resolve** and **dynamic-tunnel-attributes** options introduced in Junos OS Release 17.3R1.
- **aggregate-bandwidth** and **limit-bandwidth limit-bandwidth** options introduced in Junos OS Release 17.4R1 for MX Series, PTX Series, and QFX Series.
- **l-isis** and **l-ospf** keywords at the **protocol** option is introduced in Junos OS Release 19.1R1.
- **resolution-map** statement introduced in Junos OS Release 19.2R1-S1 on MX and PTX Series routers.

**Description**

Define a routing policy, including subroutine policies.

A **term** is a named structure in which match conditions and actions are defined. Routing policies are made up of one or more terms. Each routing policy term is identified by a term name. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks.

Each term contains a set of match conditions and a set of actions:

- Match conditions are criteria that a route must match before the actions can be applied. If a route matches all criteria, one or more actions are applied to the route.
- Actions specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

Generally, a router compares a route against the match conditions of each term in a routing policy, starting with the first and moving through the terms in the order in which they are defined, until a match is made and an explicitly configured or default action of **accept** or **reject** is taken. If none of the terms in the policy match the route, the router compares the route against the next policy, and so on, until either an action is taken or the default policy is evaluated.

If none of the match conditions of each term evaluates to true, the final action is executed. The final action is defined in an unnamed term. Additionally, you can define a default action (either **accept** or **reject**) that overrides any action intrinsic to the protocol.

The order of match conditions in a term is not relevant, because a route must match all match conditions in a term for an action to be taken.

To list the routing policies under the **[edit policy-options]** hierarchy level by **policy-statement policy-name** in alphabetical order, enter the **show policy-options** configuration command.

The statements are explained separately.
Options  

**actions**—(Optional) One or more actions to take if the conditions match. The actions are described in Configuring Flow Control Actions.

**family family-name**—(Optional) Specify an address family protocol. Specify **inet** for IPv4. Specify **inet6** for 128-bit IPv6, and to enable interpretation of IPv6 router filter addresses. For IS-IS traffic, specify **iso**. For IPv4 multicast VPN traffic, specify **inet-mvpn**. For IPv6 multicast VPN traffic, specify **inet6-mvpn**. For multicast-distribution-tree (MDT) IPv4 traffic, specify **inet-mdt**. For BGP route target VPN traffic, specify **route-target**. For traffic engineering, specify **traffic-engineering**.

**NOTE:** When family is not specified, the routing device or routing instance uses the address family or families carried by BGP. If multiprotocol BGP (MP-BGP) is enabled, the policy defaults to the protocol family or families carried in the network layer reachability information (NLRI) as configured in the family statement for BGP. If MP-BGP is not enabled, the policy uses the default BGP address family unicast IPv4.

**from**—(Optional) Match a route based on its source address.

**as-path-unique-count count (equal | orhigher | orlower)**—(Optional) Specify a number from 0 through 1024 to filter routes based on the number of unique autonomous systems (ASs) in the AS path. Specify the match condition for the unique AS path count.

**aggregate-bandwidth**—(Optional) Enable BGP to advertise aggregate outbound link bandwidth for load balancing.

**dynamic-tunnel-attributes dynamic-tunnel-attributes**—(Optional) Choose a set of defined dynamic tunnel attributes for forwarding traffic over V4oV6 tunnels.

**match-conditions**—(Optional in from statement; required in to statement) One or more conditions to use to make a match. The qualifiers are described in Routing Policy Match Conditions.

**multipath-resolve multipath-resolve**—(Optional) Enable the use of all paths for resolution over the specified prefix.

**limit-bandwidth limit-bandwidth**—(Optional) Specify the limit for advertised aggregate outbound link bandwidth for load balancing.

**Range:** 0 through 4,294,967,295 bytes

**no-entropy-label-capability**—(Optional) Disable the entropy label capability advertisement at egress or transit routes specified in the policy.

**priority (high | medium | low)**—(Optional) Configure the priority for an IS-IS route to change the default order in which the routes are installed in the routing table, in the event of a network topology change.
**policy subroutine-policy-name**—Use another policy as a match condition within this policy. The name identifying the subroutine policy can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" "). Policy names cannot take the form `.*-internal.*`, as this form is reserved. For information about how to configure subroutines, see *Understanding Policy Subroutines in Routing Policy Match Conditions*.

**policy-name**—Name that identifies the policy. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

**prefix-list prefix-list-name**—Name of a list of IPv4 or IPv6 prefixes.

**prefix-list-filter prefix-list-name**—Name of a prefix list to evaluate using qualifiers; `match-type` is the type of match, and `actions` is the action to take if the prefixes match.

**protocol protocol-name**—Name of the protocol used to control traffic engineering database import at the originating point.

Starting in Junos OS Release 19.1R1, you can specify options to match label IS-IS and label OSPF routes using the `lisis` and `l ospf` options, respectively. The `isis` options matches all IS-IS routes, excluding labelled IS-IS routes. The `ospf` option matches all OSPF routes, including OSPFv2, OSPFv3 and labelled OSPF routes.

**resolution-map**—(Optional) Set resolution map modes. A given resolution-map can be shared across multiple policy-statements.

**route-filter destination-prefix match-type <actions>**—(Optional) List of routes on which to perform an immediate match; `destination-prefix` is the IPv4 or IPv6 route prefix to match, `match-type` is the type of match (see *Configuring Route Lists*), and `actions` is the action to take if the `destination-prefix` matches.

**source-address-filter source-prefix match-type <actions>**—(Optional) Unicast source addresses in multiprotocol BGP (MBGP) and Multicast Source Discovery Protocol (MSDP) environments on which to perform an immediate match. `source-prefix` is the IPv4 or IPv6 route prefix to match, `match-type` is the type of match (see *Configuring Route Lists*), and `actions` is the action to take if the `source-prefix` matches.

**tag value**—(Optional) A numeric value that identifies a route. You can tag certain routes to prioritize them over other routes. In the event of a network topology change, Junos OS updates these routes in the routing table before updating other routes with lower priority. You can also tag some routes to identify and reject them based on your requirement.

**term term-name**—Name that identifies the term. The term name must be unique in the policy. It can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the entire name in quotation marks (" "). A policy statement can include multiple terms. We recommend that you name all terms. However, you do have the option to include an unnamed term which must be the final term in the policy. To configure an unnamed term, omit the `term` statement when defining match conditions and actions.
to—(Optional) Match a route based on its destination address or the protocols into which the route is being advertised.

then—(Optional) Actions to take on matching routes. The actions are described in Configuring Flow Control Actions and Configuring Actions That Manipulate Route Characteristics.

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

Related Documentation
• dynamic-db
• Understanding Source Packet Routing in Networking (SPRING)

pool

Syntax
pool pool-name <priority priority>;

Hierarchy Level
[edit interfaces br-pim/0/port dialer-options],
[edit interfaces umdo dialer-options],
[edit interfaces dl unit logical-unit-number dialer-options],
[edit logical-systems logical-system-name interfaces dl unit logical-unit-number dialer-options]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
On J Series Services Routers, for logical and physical ISDN interfaces, specify the dial pool. The dial pool allows logical (dialer) and physical (br-pim/0/port) interfaces to be bound together dynamically on a per-call basis. On a dialer interface, pool directs the dialer interface which dial pool to use. On br-pim/0/port interface, pool defines the pool to which the interface belongs.

Options
pool-name—Pool identifier.

priority priority—(Physical br-pim/0/port interfaces only) Specify a priority value of 0 (lowest) to 255 (highest) for the interface within the pool.

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

Related Documentation
• Junos OS Interfaces and Routing Configuration Guide
pop

Syntax  pop;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

Description  NOTE:  On EX4300 switches, pop is not supported at the [edit interfaces interface-name unit logical-unit-number input-vlan-map] hierarchy level.

For Gigabit Ethernet IQ, 10-Gigabit Ethernet IQ2, and IQ2-E interfaces; 10-Gigabit Ethernet LAN/WAN PIC; aggregated Ethernet interfaces using Gigabit Ethernet IQ interfaces; 100-Gigabit Ethernet Type 5 PIC with CFP; and Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces, specify the VLAN rewrite operation to remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.

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

Related Documentation  • Removing a VLAN Tag
• Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
pop-all-labels

Syntax

pop-all-labels {
  required-depth number;
}

Hierarchy Level

[edit interfaces interface-name atm-options mpls],
[edit interfaces interface-name sonet-options mpls],
[edit interfaces interface-name fastether-options mpls],
[edit interfaces interface-name gigether-options mpls]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description

For passive monitoring on ATM, SONET/SDH, Fast Ethernet, and Gigabit Ethernet interfaces only, removes up to two MPLS labels from incoming IP packets. For passive monitoring on T Series devices, removes up to five MPLS labels from incoming IP packets.

This statement has no effect on IP packets with more than two MPLS labels, or IP packets with more than five MPLS labels on T Series devices. Packets with MPLS labels cannot be processed by the Monitoring Services PIC; if packets with MPLS labels are forwarded to the Monitoring Services PIC, they are discarded.

The remaining statement is explained separately. See CLI Explorer.

Default

If you omit this statement, the MPLS labels are not removed, and the packet is not processed by the Monitoring Services PIC.

Required Privilege Level

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

Related Documentation

• Removing MPLS Labels from Incoming Packets
• Enabling Packet Flow Monitoring on SONET/SDH Interfaces
• Junos OS Services Interfaces Library for Routing Devices
pop-pop

Syntax  pop-pop;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  For Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, and 100-Gigabit Ethernet Type 5 PIC with CFP, and for 10-Gigabit Ethernet SFP interfaces on EX Series switches, specify the VLAN rewrite operation to remove both the outer and inner VLAN tags of the frame.

Required Privilege

Level  interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation

• Removing the Outer and Inner VLAN Tags
pop-swap

Syntax

```
pop-swap;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]
```

Release Information

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the VLAN rewrite operation to remove the outer VLAN tag of the frame, and replace the inner VLAN tag of the frame with a user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.

You can use this statement on Gigabit Ethernet IQ, IQ2, IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, and 100-Gigabit Ethernet Type 5 PIC with CFP.

Required Privilege Level

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

Related Documentation

- Removing the Outer VLAN Tag and Rewriting the Inner VLAN Tag
**port**

**Syntax**
```
port {
    minimum port-number;
    maximum port-number;
}
```

**Hierarchy Level**
```
[edit interfaces vsp-fpc/pic/port unit logical-unit-number compression rtp]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For voice services interfaces only, assign User Datagram Protocol (UDP) destination port numbers reserved for Real-Time Transport Protocol (RTP) traffic.

**Options**
- **minimum port-number**—Specify minimum port number.
  - **Range:** 0 through 65,535
- **maximum port-number**—Specify maximum port number.
  - **Range:** 0 through 65,535

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

**Related Documentation**
- Junos OS Services Interfaces Library for Routing Devices
port-priority

Syntax  
port-priority priority;

Hierarchy Level  
[edit interfaces interface-name gigether-options 802.3ad lacp]

Release Information  
Statement introduced in Junos OS Release 9.3.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.  
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

Description  
Define LACP port priority at the interface level.

Options  
priority—Priority for being elected to be the active port and both collect and distribute traffic. A smaller value indicates a higher priority for being elected.

Range: 0 through 65535
Default: 127

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

Related Documentation  
• Configuring LACP Link Protection of Aggregated Ethernet Interfaces for Switches
• Configuring Aggregated Ethernet LACP (CLI Procedure)
port-status-tlv

Syntax  port-status-tlv blocked;

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management action-profile tlv-action event]
                  [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]


Description  Define an action-profile consisting of various events and the action. Based on values of port-status-tlv in the received CCM packets, specific action such as interface-down can be taken using action-profile options.

Options  blocked—When the incoming CCM packet contains port status TLV with value blocked, the action will be triggered for this action-profile.

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

Related Documentation  • Configuring a CFM Action Profile to Specify CFM Actions for CFM Events
                      • Configuring Remote MEP Action Profile Support
**post-service-filter**

**Syntax**
```
post-service-filter filter-name;
```

**Hierarchy Level**
- `edit interfaces interface-name unit logical-unit-number family inet service input`
- `edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service input`

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Define the filter to be applied to traffic after service processing. The filter is applied only if a service set is configured and selected.

**Options**
- `filter-name`—Identifier for postservice filter.

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

**Related Documentation**
- *Junos OS Services Interfaces Library for Routing Devices*
ppp-options

Syntax

```plaintext
ppp-options {
  authentication [ authentication-protocols ];
  mru size;
  mtu (size | use-lower-layer);
  chap {
    access-profile name;
    challenge-length minimum minimum-length maximum maximum-length;
    default-chap-secret name;
    local-name name;
    passive;
  }
  compression {
    acfc;
    pfc;
  }
  dynamic-profile profile-name;
  initiate-ncp (ip | ipv6 | dual-stack-passive)
  ipcp-suggest-dns-option;
  lcp-max-conf-req number
  lcp-restart-timer milliseconds;
  loopback-clear-timer seconds;
  ncp-max-conf-req number
  ncp-restart-timer milliseconds;
  on-demand-ip-address
  pap {
    access-profile name;
    default-pap-password password;
    local-name name;
    local-password password;
    passive;
  }
}
```

Hierarchy Level

- [edit interfaces interface-name],
- [edit interfaces interface-name unit logical-unit-number],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

On interfaces with PPP encapsulation, configure PPP-specific interface properties.

For ATM2 IQ interfaces only, you can configure CHAP on the logical interface unit if the logical interface is configured with one of the following PPP over ATM encapsulation types:

- atm-ppp-llc—PPP over AAL5 LLC encapsulation.
- atm-ppp-vc-mux—PPP over AAL5 multiplex encapsulation.
**BEST PRACTICE:** On inline service (si) interfaces for L2TP, only the chap and pap statements are typically used for subscriber management. We recommend that you leave the other statements subordinate to ppp-options—including those subordinate to chap and pap—at their default values.

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**
- Configuring the PPP Challenge Handshake Authentication Protocol on page 121
- Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface
**pppoe-options**

**Syntax**

```
pppoe-options {
  access-concentrator name;
  auto-reconnect seconds;
  (client | server);
  service-name name;
  underlying-interface Interface-name;
  ppp-max-payload ppp-max-payload
}
```

**Hierarchy Level**

```
[edit interfaces pp0 unit logical-unit-number],
[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number]
[set interface ppp interface unit logical-unit-number ppp-max-payload ppp-max-payload],
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
client Statement introduced in Junos OS Release 8.5.
server Statement introduced in Junos OS Release 8.5.
**ppp-max-payload** Statement introduced in Junos OS Release 15.1X49-D100.

**Description**

Configure PPP over Ethernet-specific interface properties.

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 maximum payload allowed on an Ethernet frame is 1500 bytes. For a PPPoE interface, the PPPoE header uses 6 bytes and the PPP protocol ID uses 2 bytes. This restricts the maximum MTU size on a PPPoE interface to 1492 bytes, which can cause frequent fragmentation and reassembly of larger PPP packets received over the PPPoE interface. To prevent frequent fragmentation and reassembly for PPP packets over Ethernet, you can configure the maximum transmission unit (MTU) and MRU sizes for PPP subscribers.

For PPPoE subscribers, the PPP MRU or PPP MTU size can be greater than 1492 bytes if the PPP-Max-Payload tag is received in the PPPoE Active Discovery Request (PADR) packets.

The PPP-Max-Payload option allows you to override the default behavior of the PPPoE client by providing a maximum size that the PPP payload can support in both sending and receiving directions. The PPPoE server might allow the negotiation of an MRU larger than 1492 octets and the ability to use an MTU larger than 1500 octets.

It is important to set an appropriate value for the MTU size of the physical interface before setting ppp-max-payload. The value of mtu must be greater than the value of ppp-max-payload.

To enable Jumbo frames refer Understanding Jumbo Frames Support for Ethernet Interfaces.
Required Privilege Level

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

Related Documentation

- Configuring a PPPoE Interface

**pppoe-underlying-options (Static and Dynamic Subscribers)**

**Syntax**

```plaintext
pppoe-underlying-options {
    access-concentrator name;
    dynamic-profile profile-name;
    direct-connect
    duplicate-protection;
    max-sessions number;
    max-sessions-vsa-ignore;
    service-name-table table-name;
    short-cycle-protection <lockout-time-min minimum-seconds> <lockout-time-max maximum-seconds> <filter [aci]>
}
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced in Junos OS Release 10.0.

**Description**

Configure PPPoE-specific interface properties for the underlying interface on which the router creates a static or dynamic PPPoE logical interface. The underlying interface must be configured with PPPoE (ppp-over-ether) encapsulation.

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

- Configuring PPPoE (for static interfaces)
- Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces
- Assigning a Service Name Table to a PPPoE Underlying Interface
preferred

Syntax  preferred;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family family address address],
 [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address 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 this address to be the preferred address on the interface. If you configure more
 than one address on the same subnet, the preferred source address is chosen by default
 as the source address when you initiate frame transfers to destinations on the subnet.

NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Default  The lowest-numbered address on the subnet is the preferred address.

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 Address on page 191
preferred-source-address

Syntax

preferred-source-address address;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family unnumbered-address interface-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family unnumbered-address interface-name]

Release Information

Statement introduced in Junos OS Release 9.0.

Description

For unnumbered Ethernet interfaces configured with a loopback interface as the donor interface, specify one of the loopback interface's secondary addresses as the preferred source address for the unnumbered Ethernet interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network.

Configuration of a preferred source address for unnumbered Ethernet interfaces is supported for the IPv4 and IPv6 address families.

Options

address—Secondary IP address of the donor loopback interface.

Required Privilege Level

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

Related Documentation

- Configuring a Preferred Source Address for Unnumbered Ethernet or Demux Interfaces on page 202
- address on page 407
- Junos OS Administration Library
preferred-source-address

**Syntax**

preferred-source-address address;

**Hierarchy Level**

[edit dynamic-profiles interfaces interface-name unit logical-unit-number family family unnumbered-address interface-name],
[edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family family],

**Release Information**

Statement introduced in Junos OS Release 9.2.
Support for the $junos-preferred-source-address and $junos-preferred-source-ipv6-address predefined variables introduced in Junos OS Release 9.6.

**Description**

For unnumbered Ethernet interfaces configured with a loopback interface as the donor interface, specify one of the loopback interface's secondary addresses as the preferred source address for the unnumbered Ethernet interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network. To configure the preferred source address dynamically, instead of using this statement, you must include the $junos-preferred-source-address predefined variable for IPv4 (family inet) addresses or the $junos-preferred-source-ipv6-address predefined variable for IPv6 (family inet6) addresses.

Configuration of a preferred source address for unnumbered Ethernet interfaces is supported for IPv4 and IPv6 address families.

---

### NOTE:

When you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the $junos-routing-instance predefined variable, you must not configure a preferred source address, whether with the $junos-preferred-source-address predefined variable, the $junos-preferred-source-ipv6-address predefined variable, or the preferred-source-address statement. Configuring the preferred source address in this circumstance causes a commit failure.

---

**Options**

- **address**—Secondary IP address of the donor loopback interface. Alternatively, use the $junos-preferred-source-address or the $junos-preferred-source-ipv6-address predefined variable to dynamically apply a preferred source address to the unnumbered Ethernet interface.

**Required Privilege Level**

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

- Configuring an Unnumbered Interface on page 202
- Junos OS Network Interfaces Library for Routing Devices
- Junos OS Administration Library
premium (Hierarchical Policer)

Syntax

```
premium {
  if-exceeding {
    bandwidth-limit bandwidth;
    burst-size-limit burst;
  }
  then {
    discard;
  }
}
```

Hierarchy Level

```
[edit dynamic-profiles profile-name firewall hierarchical-policer],
[edit firewall hierarchical-policer]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Support at the [edit dynamic-profiles ... hierarchical-policer name] hierarchy level introduced in Junos OS Release 11.4.

Description

On M40e, M120, and M320 edge routers with FPC input as FFPC and FPC output as SFPC, and on MX Series, T320, T640, and T1600 edge routers with Enhanced Intelligent Queuing (IQE) PICs, T4000 routers with Type 5 FPC and Enhanced Scaling Type 4 FPC, specify a premium level for a hierarchical policer.

Options

Options are described separately.

Required Privilege

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

Related Documentation

- Applying Policers on page 210
- Guidelines for Applying Traffic Policers
- Hierarchical Policer Configuration Overview
- Hierarchical Policers
- aggregate (Hierarchical Policer)
- bandwidth-limit (Hierarchical Policer) on page 442
- burst-size-limit (Hierarchical Policer) on page 455
- hierarchical-policer
- if-exceeding (Hierarchical Policer) on page 656
premium (Output Priority Map)

Syntax

```plaintext
premium {
  forwarding-class class-name {
    loss-priority (high | low);
  }
}
```

Hierarchy Level

[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile output-priority-map classifier]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For Gigabit Ethernet IQ interfaces only, define the classifier for egress premium traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Specifying an Output Priority Map
- input-priority-map on page 682
premium (Policer)

Syntax

```plaintext
premium {
  bandwidth-limit bps;
  burst-size-limit bytes;
}
```

Hierarchy Level

```plaintext
[edit interfaces interface-name gigether-options ethernet-switch-profile ethernet-policer-profile policer cos-policer-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define a policer to apply to nonpremium traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- Configuring Gigabit Ethernet Policers
- aggregate (Gigabit Ethernet CoS Policer) on page 412
- ieee802.1p on page 655
**preserve-interface**

**Syntax**  
`preserve-interface;`

**Hierarchy Level**  
[edit interfaces interface-name sonet-options aps]

**Release Information**  
Statement introduced in Junos OS Release 7.6.

**Description**  
Provide link PIC replication, providing MLPPP link redundancy at the port level. This feature is supported with SONET APS and the following link PICs:

- Channelized OC3 IQ PIC
- Channelized OC12 IQ PIC
- Channelized STM1 IQ PIC

Link PIC replication provides the ability to add two sets of links, one from the active SONET PIC and the other from the standby SONET PIC, to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without triggering link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation.

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

**Related Documentation**  
- Configuring Link PIC Redundancy
- Junos OS Services Interfaces Library for Routing Devices
primary (Address on Interface)

Syntax primary;

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


Description Configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.

NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Default For unicast traffic, the primary address is the lowest non-127 (in other words, non-loopback) preferred address on the unit.

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 Address on page 191
primary (Interface for Router)

Syntax

primary;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family ]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family ]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the primary interface for a device. By default, the multicast-capable interface with the lowest-index address is chosen as the primary interface. If there is no such interface, the point-to-point interface with the lowest-index address is chosen. Otherwise, any interface with an address can be picked. In practice, this means that, on the device, the fxp0 or em0 interface is picked by default. To configure a different interface to be the primary interface, you include this statement.

The primary interface for the router has the following characteristics:

- It is the interface through which the packets go out when you type a command such as ping 255.255.255.255—that is, a command that does not include an interface name (there is no interface type-0/0/0.0 qualifier) and where the destination address does not imply any particular outgoing interface.

- It is the interface on which multicast applications running locally on the router, such as Session Announcement Protocol (SAP), perform group joins by default.

- It is the interface from which the default local address is derived for packets sourced out of an unnumbered interface if there are no non-127 addresses configured on the loopback interface, lo0.

Required Privilege Level

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

Related Documentation

- Configuring Default, Primary, and Preferred Addresses and Interfaces on page 193
primary (AS PIC or Multiservices PIC Interfaces)

Syntax: primary interface-name;

Hierarchy Level: [edit interfaces (rsp0 | rsp1) redundancy-options]

Release Information: Statement introduced before Junos OS Release 7.4.

Description: Specify the primary AS PIC or MultiServices PIC interface.

Options: 
- **interface-name**—The identifier for the AS PIC interface or MultiServices PIC interface, which must be of the form sp-fpc/pic/port.

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

Related Documentation:
- Junos OS Services Interfaces Library for Routing Devices
priority (OAM Connectivity-Fault Management)

Syntax

priority number;

Hierarchy Level

[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name mep mep-id]

For EX Series Switches:

[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]

Release Information

Statement introduced in Junos OS Release 8.4.

Description

IEEE 802.1p priority bits used by the continuity check messages.

Options

number—Configure the IEEE 802.1p priority bits to be used in the VLAN header of the CFM packets.

Range: 0 through 7

Required Privilege

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring a MEP to Generate and Respond to CFM Protocol Messages
priority (Schedulers)

Syntax
priority (high | low);

Hierarchy Level
[edit interfaces at-fpc/pic/port atm-options scheduler-maps map-name forwarding-class class-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For ATM2 IQ interfaces only, assign queuing priority to a forwarding class.

Options
- low—Forwarding class has low priority.
- high—Forwarding class has high priority.

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

Related Documentation
- ATM2 IQ VC Tunnel CoS Components Overview
promiscuous-mode

Syntax

promiscuous-mode {
    vpi vpi-identifier;
}

Hierarchy Level
[edit interfaces interface-name atm-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description
For ATM interfaces with atm-ccc-cell-relay encapsulation, map all incoming cells from either an interface port or a VP to a single label-switched path (LSP) without restricting the VCI number. Promiscuous mode allows you to map traffic from all 65,535 VCIs to a single LSP, or from all 256 VPIs to a single LSP.

NOTE: In ACX Series routers, the statement supports only Inverse Multiplexing for ATM (IMA).

Options
vpi-identifier—Open this VPI in promiscuous mode.

Range: 0 through 255

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

Related Documentation
• Configuring ATM Cell-Relay Promiscuous Mode
• vpi (ATM CCC Cell-Relay Promiscuous Mode) on page 1137
protect-circuit

Syntax: protect-circuit group-name;

Hierarchy Level: [edit interfaces interface-name sonet-options aps]

Release Information: Statement introduced before Junos OS Release 7.4.

Description: Configure the protect router in an APS circuit pair. When the working interface fails, APS brings up the protection circuit and the traffic is moved to the protection circuit.

Options: group-name—Circuit’s group name.

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

Related Documentation:
- Configuring Basic Automatic Protect Switching
- working-circuit on page 1148
protection-group

Syntax

protection-group {
  ethernet-ring ring-name {
    data-channel {
      vlan number
    }
    east-interface {
      control-channel channel-name {
        vlan number;
        interface name interface-name
      }
    }
    guard-interval number;
    node-id mac-address;
    restore-interval number;
    ring-protection-link-owner;
    non-revertive;
    wait-to-block-interval number;
    major-ring-name name;
    propagate-tc;
    compatibility-version (1|2);
    ring-id number;
    non-vc-mode;
    dot1p-priority number;
    west-interface {
      control-channel channel-name {
        vlan number;
        interface name interface-name
      }
      virtual-control-channel {
        west-interface name;
        east-interface name;
      }
    }
  }
}

control-vlan (vlan-id | vlan-name);

east-interface {
  node-id mac-address;
  control-channel channel-name {
    vlan number;
    interface name interface-name
  }
  interface-none
  ring-protection-link-end;
}

data-channel {

vlan number
}
guard-interval number;
node-id mac-address;
restore-interval number;
ring-protection-link-owner;
west-interface {
    node-id mac-address;
    control-channel channel-name {
        vlan number;
        interface name interface-name
    }
    interface-none
    ring-protection-link-end;
}
control-channel channel-name {
    vlan number;
    interface name interface-name
}
}
guard-interval number;
restore-interval number;
traceoptions {
    file filename <no-stamp> <world-readable | no-world-readable> <replace> <size size>;
    flag flag;
}
}

Hierarchy Level [edit protocols]

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure Ethernet ring protection switching.
The statements are explained separately. All statements apply to MX Series routers. EX Series switches do not assign node-id and use control-vlan instead of control-channel.

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

Syntax  protocol-down;

Hierarchy Level  [edit protocols oam ethernet link-fault-management action-profile event]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Upper layer indication of protocol down event. When the protocol-down statement is included, the protocol down event triggers the action specified under the action statement.

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

Related Documentation  • Configuring an OAM Action Profile
protocols

**Syntax**
protocols [inet isompls];

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number family tcc]

**Release Information**
Statement introduced in Junos OS Release 8.3.

**Description**
For Layer 2.5 VPNs on T Series, MX Series, M120, and M320 routers support, configure IS-IS (ISO traffic) or MPLS traffic to traverse a TCC interface. By default, IPv4 (inet) traffic runs on T Series, MX, Series, M120, and M320 routers and over TCC interfaces. You must configure the same traffic type on both ends of the Layer 2.5 VPN.

NOTE: Some platform and FPC combinations cannot pass TCC encapsulated ISO traffic. See Platforms/FPCs That Cannot Forward TCC Encapsulated ISO Traffic for details.

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

**Related Documentation**
- Configuring IS-IS or MPLS Traffic for TCC Interfaces on page 262
- Platforms/FPCs That Cannot Forward TCC Encapsulated ISO Traffic
proxy

Syntax
proxy inet-address address;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For Layer 2.5 VPNs using an Ethernet interface as the TCC router, configure the IP address for which the TCC router is proxying. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only. Ethernet TCC is not supported on the T640 router.

Options
inet-address—Configure the IP address of the neighbor to the TCC router.

Required Privilege
level

Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
- Configuring Translation Cross-Connect Interface Switching
- Example: Configuring an Ethernet TCC or Extended VLAN TCC
- remote on page 953
- Junos OS VPNs Library for Routing Devices
**proxy-arp**

**Syntax**  
proxy-arp (restricted | unrestricted);

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

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.6 for EX Series switches.  
**restricted** added in Junos OS Release 10.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.2 for the QFX Series.

**Description**  
For Ethernet interfaces only, configure the router or switch to respond to any ARP request, as long as the router or switch has an active route to the ARP request’s target address.

---

**NOTE:** You must configure the IP address and the inet family for the interface when you enable proxy ARP.

---

**Default**  
Proxy ARP is not enabled. The router or switch responds to an ARP request only if the destination IP address is its own.

**Options**  
- **none**—The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.
- **restricted**—(Optional) The router or switch responds to ARP requests in which the physical networks of the source and target are different and does not respond if the source and target IP addresses are in the same subnet. The router or switch must also have a route to the target IP address.
- **unrestricted**—(Optional) The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.

**Default:** unrestricted

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

**Related Documentation**  
- Configuring Restricted and Unrestricted Proxy ARP
- Configuring Proxy ARP on Switches
- Example: Configuring Proxy ARP on an EX Series Switch
- Configuring Gratuitous ARP

---
push

Syntax
push;

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

Description
NOTE: On EX4300 switches, push is not supported at the [edit interfaces interface-name unit logical-unit-number output-vlan-map] hierarchy level.

Specify the VLAN rewrite operation to add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag.

You can use this statement on Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces; 10-Gigabit Ethernet LAN/WAN PIC; aggregated Ethernet interfaces using Gigabit Ethernet IQ interfaces; 100-Gigabit Ethernet Type 5 PIC with CFP; and Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces.

If you include the push statement in the configuration, you must also include the pop statement at the [edit interfaces interface-name unit logical-unit-number output-vlan-map] hierarchy level.

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

Related Documentation
• Stacking a VLAN Tag
• Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
**push-push**

**Syntax**

```
push-push;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]
```

**Release Information**


**Description**

Specify the VLAN rewrite operation to push two VLAN tags in front of the frame.

You can use this statement on Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, on aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, and 100-Gigabit Ethernet Type 5 PIC with CFP.

**Required Privilege Level**

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

**Related Documentation**

- *Stacking Two VLAN Tags*
queue-depth

Syntax
queue-depth cells;

Hierarchy Level
[edit interfaces interface-name atm-options linear-red-profiles profile-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For ATM2 IQ interfaces only, define maximum queue depth in the CoS VC drop profile. Packets are always dropped beyond the defined maximum. This statement is mandatory; there is no default configuration.

Default
Buffer usage is unregulated.

Options
 cells—Maximum number of cells the queue can contain.
 Range: 1 through 64,000 cells

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

Related Documentation
• ATM2 IQ VC Tunnel CoS Components Overview
• Configuring Linear RED Profiles on ATM Interfaces
• high-plp-threshold on page 637
• low-plp-threshold on page 768
queue-length

Syntax

queue-length number;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ],
[edit interfaces interface-name unit logical-unit-number shaping ],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number shaping ]

Release Information

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

Description

For ATM1 interfaces only, define the maximum queue length in the traffic-shaping profile.
For ATM1 PICs, each VC has its own independent shaping parameters.

Default

Buffer usage is unregulated.

Options

number—Maximum number of packets the queue can contain.
Range: 1 through 16,383 packets
Default: 16,383 packets

Required Privilege Level

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

Related Documentation

• Configuring the ATM1 Queue Length
queues

Syntax  queues [ queue-numbers ];

Hierarchy Level  [edit interfaces vsp-fpc/pic/port unit logical-unit-number compression rtp ]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For voice services interfaces only, assign queue numbers for RTP traffic.

Options  queues queue-numbers—Assign one or more of the following queues: q0, q1, q2, q3. For VRRP services, specify the q3 option instead of q0.

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

Related Documentation  • Junos OS Services Interfaces Library for Routing Devices
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  
• Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch
radius-realm

Syntax  
radius-realm radius-realm-string;

Hierarchy Level  
[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include]

Release Information  
Statement introduced in Junos OS Release 10.0.

Description  
Specify that the user-defined RADIUS realm string is appended as a last piece to the
username and used by RADIUS to direct the authentication request to a profile that does
not allocates addresses.

Options  
radius-realm-string—A string to describe the RADIUS realm.

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

Related Documentation  
• Configuring VLAN Interface Username Information for AAA Authentication
ranges (Dynamic Stacked VLAN)

Syntax:
ranges (any | low-tag–high-tag), (any | low-tag–high-tag);

Hierarchy Level:
[edit interfaces interface-name auto-configure stacked-vlan-ranges dynamic-profile profile-name]

Release Information:
Statement introduced in Junos OS Release 9.5.

Description:
Configure VLAN ranges for dynamic, auto-sensed stacked VLANs.

Options:
- any—The entire VLAN range.
- low-tag—The lower limit of the VLAN range.
- high-tag—The upper limit of the VLAN range.

Range: 1 through 4094

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

Related Documentation:
- Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANS
ranges (Dynamic VLAN)

Syntax
ranges (any | low-tag)-(any | high-tag);

Hierarchy Level
[edit interfaces interface-name auto-configure vlan-ranges dynamic-profile profile-name]

Release Information
Statement introduced in Junos OS Release 9.5.

Description
Configure VLAN ranges for dynamic, auto-sensed VLANs.

Options
any—The entire VLAN range.
  low-tag—The lower limit of the VLAN range.
  high-tag—The upper limit of the VLAN range.

Range: 1 through 4094

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

Related Documentation
• Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs
rate

Syntax  rate percentage;

Hierarchy Level  [edit interfaces interface-name receive-bucket],
                 [edit interfaces interface-name transmit-bucket]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Specify percentage of the interface line rate that is available to receive or transmit packets.

Options  percentage—Percentage of the interface line rate that is available to receive or transmit packets.

          Range: 0 through 100

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

Related Documentation  • Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140
rate

Syntax  
rate new-sessions-per-second;

Hierarchy Level  
[edit interfaces interface-name services-options session-limit]

Release Information  
Statement introduced in Junos OS Release 9.6. Support added in Junos OS Release 19.3R1 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-MX-SPC3 services card.

Description  
Specify the maximum number of new sessions allowed per second on services cards.

Options  
rate new-sessions-per-second—Specify the maximum number of new sessions allowed per second.
   Range: 0, which indicates no limit, and 500 or greater.

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

Related Documentation  
• How to Configure Services Interfaces for Next Gen Services

rdi

Syntax  
rdi;

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management action-profile tlv-action event]

Release Information  
Statement introduced in Junos OS Release 10.1.

Description  
Define a new event rdi. The remote defect indication (rdi) event is triggered whenever CCM packets are received from a remote location with the rdi bit set.
This event is cleared and action is reverted when none of the remote MEPs send the CCM packets with the RDI bit.

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

Related Documentation  
• Configuring a CFM Action Profile to Specify CFM Actions for CFM Events
**reassemble-packets**

**Syntax**
```
reassemble-packets;
```

**Hierarchy Level**

```
[edit interfaces gr-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces gr-fpc/pic/port unit logical-unit-number]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.

**Description**
Enable reassembly of fragmented tunnel packets on generic routing encapsulation (GRE) tunnel interfaces.

**Required Privilege Level**

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

**Related Documentation**

- Junos OS Services Interfaces Library for Routing Devices
- Configuring Packet Reassembly
reauthentication

Syntax  
reauthentication (disable | interval seconds);

Hierarchy Level  
[edit protocols dot1x authenticator interface interface-id]

Release Information  
Statement introduced in Junos OS Release 9.3.

Description  
Set or disable the periodic reauthentication of the client.

Options  
• disable—Disable the periodic reauthentication of the client.
  • interval seconds—Specify the periodic reauthentication time interval.

  Range: 1 through 65,535 seconds
  Default: 3600 seconds

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

Related Documentation  
• IEEE 802.1x Port-Based Network Access Control Overview
  • dot1x on page 534
  • interface (IEEE 802.1x) on page 687
  • quiet-period on page 940
receive-bucket

Syntax

receive-bucket {
  overflow (discard | tag);
  rate percentage;
  threshold bytes;
}

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Set parameters for the receive leaky bucket, which specifies what percentage of the interface’s total capacity can be used to receive packets.

For each DS3 channel on a channelized OC12 interface, you can configure a unique receive bucket.

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 Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140
• transmit-bucket on page 1076
receive-options-packets

Syntax
receive-options-packets;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For a Monitoring Services PIC and an ATM or SONET/SDH PIC installed in an M160, M40e, or T Series router, guarantee conformity with cflowd records structure. This statement is required when you enable passive monitoring.

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

Related Documentation
- Enabling Passive Monitoring on ATM Interfaces
- Enabling Packet Flow Monitoring on SONET/SDH Interfaces

receive-ttl-exceeded

Syntax
receive-ttl-exceeded;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For Monitoring Services PIC and an ATM or SONET/SDH PIC installed in an M160, M40e, or T Series router, guarantee conformity with cflowd records structure. This statement is required when you enable passive monitoring.

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

Related Documentation
- Enabling Passive Monitoring on ATM Interfaces
- Enabling Packet Flow Monitoring on SONET/SDH Interfaces
red-differential-delay

Syntax  
red-differential-delay milliseconds;

Hierarchy Level  
[edit interfaces interface-name mlfr-uni-nni-bundle-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For link services and voice services interfaces only, configure the red differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.

Options  
milliseconds—Red differential delay threshold.
Range: 1 through 2000 milliseconds
Default: 10 milliseconds

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

Related Documentation  
- action-red-differential-delay on page 404
- yellow-differential-delay on page 1149
- Junos OS Services Interfaces Library for Routing Devices
redial-delay

Syntax  redial-delay time;

Hierarchy Level  [edit interfaces dln unit logical-unit-number dialer-options],
                   [edit logical-systems logical-system-name interfaces dln unit logical-unit-number
dialer-options]

Release Information  Statement introduced in Junos OS Release 7.5.

Description  On J Series Services Routers with interfaces configured for ISDN with dialout, specify the
delay (in seconds) between two successive calls made by the dialer. To configure callback
mode, include the callback statement at the [edit interfaces dln unit logical-unit-number
dialer-options] hierarchy level.

If the callback statement is configured, you cannot use the caller caller-id statement at
the [edit interfaces dln unit logical-unit-number dialer-options] hierarchy level.

Options  time—Delay (in seconds) between two successive calls.
  Range:  2 through 255 seconds
  Default:  3 seconds

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

Related Documentation  • ISDN Interfaces Overview
  • Junos OS Interfaces and Routing Configuration Guide
## redundancy-options

**Syntax**

```plaintext
redundancy-options {
  primary interface-name;
  secondary interface-name;
  hot-standby;
}
```

**Hierarchy Level**

- `[edit interfaces (rsp0 | rsp1)]`,
- `[edit interfaces rlsqnumber]`
- `[edit interfaces rspnumber]`
- `[edit interfaces rmsnumber]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Specify the primary and secondary (backup) AS PIC interfaces or MultiServices PIC interfaces.

**Options**

- **primary interface-name**—The identifier for the primary LSQ AS, rsp, or rms interface.
- **secondary interface-name**—The identifier for the secondary (backup) LSQ AS, rsp, or rms interface.
- **hot-standby**—For one-to-one AS, rsp, or rms redundancy configurations, specify that the failure detection and recovery must take place in less than 5 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 Services Interfaces Library for Routing Devices*
remote

Syntax  
remote {
    (inet-address address | mac-address address);
}

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

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For Layer 2.5 VPNs using an Ethernet interface as the TCC router, configure the location of the remote router. Ethernet TCC is supported on interfaces that carry IPv4 traffic only. Ethernet TCC encapsulation is supported on 1-port Gigabit Ethernet, 2-port Gigabit Ethernet, 4-port Gigabit Ethernet, and 4-port Fast Ethernet PICs only.

Options  
mac-address—Configure the MAC address of the remote site.

inet-address—Configure the IP address of the remote site.

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

Related Documentation  
• Configuring Translation Cross-Connect Interface Switching
• Example: Configuring an Ethernet TCC or Extended VLAN TCC
• proxy on page 933
• Junos OS VPNs Library for Routing Devices
remote-loopback

Syntax  
remote-loopback;

Hierarchy Level  
[edit protocols oam link-fault-management interface interface-name]

Release Information  
Statement introduced in Junos OS Release 8.2.

Description  
For Ethernet interfaces on EX Series switches and M320, M120, MX Series, and T Series routers, set the remote DTE into loopback mode. Remove the statement from the configuration to take the remote DTE out of loopback mode. Used for IEEE 802.3ah Operation, Administration, and Management (OAM) support.

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

Related Documentation  
• Setting a Remote Interface into Loopback Mode
remote-loopback-respond

Syntax  
remote-loopback-respond;

Hierarchy Level  
[edit interfaces ct1-fpc/pic/port],  
[edit interfaces interface-name t1-options]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description  
For T1 interfaces only, configure the router to respond to remote loopback requests. Remote loopback requests can be from the facilities data link or inband.

NOTE:  When configuring CT1 interfaces on the 10-port Channelized E1/T1 IQE PIC, the remote-loopback-respond statement must be included at the [edit interfaces ct1-fpc/pic/port] hierarchy level.

Default  
The router does not respond to remote loop requests.

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

Related Documentation  
- Configuring the T1 Remote Loopback Response  
- feac-loop-respond on page 611  
- loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3) on page 760
remote-mep

Syntax

```
remote-mep mep-id {
    action-profile profile-name;
    sla-iterator-profile profile-name {
        data-tlv-size size;
        iteration-count count-value;
        priority priority-value;
    }
    detect-loc;
}
```

Hierarchy Level

```diff
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
    md-name maintenance-association ma-name mep mep-id]
```

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Configure the numeric identifier of the remote maintenance association end point (MEP) within the maintenance association.

Options

- **mep-id**—Numeric identifier of the MEP.

  **Range:** 1 through 8191

  The remaining statements are explained separately. See CLI Explorer.

Required Privilege

- **Configure**—To enter configuration mode.
- **Control**—To modify any configuration.

Related Documentation

- Configuring a MEP to Generate and Respond to CFM Protocol Messages
- `detect-loc`
**remove-when-no-subscribers**

**Syntax**
remove-when-no-subscribers;

**Hierarchy Level**
[edit interfaces interface-name auto-configure]

**Release Information**
Statement introduced in Junos OS Release 11.4.

**Description**
Remove subscriber VLANs automatically when no client sessions (for example, DHCP or PPPoE) exist on the VLAN.

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

**Related Documentation**
- Automatically Removing VLANs with No Subscribers

**request**

**Syntax**
request (protect | working);

**Hierarchy Level**
[edit interfaces interface-name sonet-options aps]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
Perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.

**Options**
- **protect**—Request that the circuit become the protect circuit.
- **working**—Request that the circuit become the working circuit.

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

**Related Documentation**
- Configuring Switching Between the Working and Protect Circuits
- force on page 620
required-depth

Syntax

```
required-depth number;
```

Hierarchy Level

```
[edit interfaces interface-name atm-options mpls pop-all-labels],
[edit interfaces interface-name sonet-options mpls pop-all-labels],
[edit interfaces interface-name fastether-options mpls pop-all-labels],
[edit interfaces interface-name gigether-options mpls pop-all-labels]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description

For passive monitoring on ATM and SONET/SDH interfaces only, specify the number of MPLS labels an incoming packet must have for the `pop-all-labels` statement to take effect.

If you include the `required-depth 1` statement, the `pop-all-labels` statement takes effect for incoming packets with one label only. If you include the `required-depth 2` statement, the `pop-all-labels` statement takes effect for incoming packets with two labels only.

Options

```
number—Number of MPLS labels on incoming IP packets.
Range: 1 or 2 labels
Default: If you omit this statement, the `pop-all-labels` statement takes effect for incoming packets with one or two labels. The default is equivalent to including the `required-depth [1 2]` statement.
```

Required Privilege Level

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

Related Documentation

- Removing MPLS Labels from Incoming Packets
- Enabling Packet Flow Monitoring on SONET/SDH Interfaces
- Junos OS Services Interfaces Library for Routing Devices
**restore-interval**

**Syntax**  
```restore-interval number;```  

**Hierarchy Level**  
```[edit protocols protection-group ethernet-ring ring-name]```  

**Release Information**  
Statement introduced in Junos OS Release 9.4.  
Statement introduced in Junos OS Release 12.1 for EX Series switches.  

**Description**  
Configures the number of minutes that the node does not process any Ethernet ring protection (ERP) protocol data units (PDUs). This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

**Options**  
- `number`—Specify the restore interval.  
  **Range:** 1 through 12 minutes

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

**Related Documentation**  
- *Ethernet Ring Protection Switching Overview*  
- *Example: Configuring Ethernet Ring Protection Switching on EX Series Switches*  
- *Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS*  
- *Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)*
retries

Syntax    retries integer;

Hierarchy Level    [edit protocols dot1x authenticator interface interface-id]

Release Information    Statement introduced in Junos OS Release 9.3.

Description    Set a limit on the number of failed authentication attempts between a port and a client. When the limit is exceeded, the port waits to reattempt authentication for the number of seconds set by the quiet-period statement configured at the same hierarchy level.

Options    integer—Specify the number of retries.

       Range: 1 through 10
       Default: 3 retries

Required Privilege Level

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

Related Documentation

       • IEEE 802.1x Port-Based Network Access Control Overview
       • dot1x on page 534
       • interface (IEEE 802.1x) on page 687
       • quiet-period on page 940
revert-time (Interfaces)

Syntax  revert-time seconds;

Hierarchy Level  [edit interfaces interface-name sonet-options aps]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure APS revertive mode.

Default  APS operates in nonrevertive mode.

Options  seconds—Amount of time to wait after the working circuit has again become functional before making the working circuit active again.

Range: 1 through 65,535 seconds
Default: None (APS operates in nonrevertive mode)

Required Privilege

Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring Revertive Mode
**revertive**

**Syntax**  
revertive;

**Hierarchy Level**  
[edit interfaces aeX aggregated-ether-options lACP link-protection]

**Release Information**  
Statement introduced in Junos OS Release 9.3.  
Statement introduced in Junos OS Release 12.3 for EX Series switches.  
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

**Description**  
Enable the ability to switch to a better priority link (if one is available).

---

**NOTE:** By default, LACP link protection is revertive. However, you can use this statement to define a specific aggregated Ethernet interface as revertive to override a global non-revertive statement specified at the [edit chassis] hierarchy level.

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

**Related Documentation**  
- [non-revertive (Chassis)]  
- [Configuring LACP Link Protection of Aggregated Ethernet Interfaces for Switches]
rfc-2615

Syntax  rfc-2615;

Hierarchy Level  [edit interfaces interface-name sonet-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Include this statement to enable features described in RFC 2615, PPP over SONET/SDH.

Default  Settings required by RFC 1619, PPP over SONET/SDH.

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

Related Documentation  • Configuring PPP Support on SONET/SDH Interfaces

ring-protection-link-end

Syntax  ring-protection-link-end;

Hierarchy Level  [edit protocols protection-group ethernet-ring ring-name (east-interface | west-interface)]

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description  Specify that the port is one side of a ring protection link (RPL) by setting the RPL end flag.

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

Related Documentation  • Ethernet Ring Protection Switching Overview  
  • Example: Configuring Ethernet Ring Protection Switching on EX Series Switches  
  • Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series 
    Switches Supporting ELS  
  • Configuring Ethernet Ring Protection Switching on Switches (CLI Procedure)
**ring-protection-link-owner**

**Syntax**

```plaintext
ring-protection-link-owner;
```

**Hierarchy Level**

```
[edit protocols protection-group ethernet-ring ring-name]
```

**Release Information**

- Statement introduced in Junos OS Release 9.4.
- Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Specify the ring protection link (RPL) owner flag in the Ethernet protection ring. Include this statement only once for each ring (only one node can function as the RPL owner).

**Required Privilege Level**

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

**Related Documentation**

- Ethernet Ring Protection Switching Overview
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
**routing-instance**

**Syntax**
```
routing-instance {
    destination routing-instance-name;
}
```

**Hierarchy Level**
- [edit interfaces interface-name unit logical-unit-number tunnel],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel]

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
To configure interfaces and logical-systems, specify the destination routing instance that points to the routing table containing the tunnel destination address.

**Default**
The default Internet routing table is inet.0.

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

**Related Documentation**
- Junos OS Services Interfaces Library for Routing Devices
**Routing-Instance (PPPoE Service Name Tables)**

**Syntax**
```
routing-instance routing-instance-name;
```

**Hierarchy Level**
```
[edit protocols pppoe service-name-tables table-name service service-name],
[edit protocols pppoe service-name-tables table-name service service-name agent-specifier
aci circuit-id-string ari remote-id-string]
```

**Release Information**
Statement introduced in Junos OS Release 10.2.

**Description**
Use in conjunction with the `dynamic-profile` statement at the same hierarchy levels to specify the routing instance in which to instantiate a dynamic PPPoE interface. You can associate a routing instance with a named service entry, empty service entry, or any service entry configured in a PPPoE service name table, or with an agent circuit identifier/agent remote identifier (ACI/ARI) pair defined for these services.

The routing instance associated with a service entry in a PPPoE service name table overrides the routing instance associated with the PPPoE underlying interface on which the dynamic PPPoE interface is created.

If you include the `routing-instance` statement at the [edit protocols pppoe service-name-tables table-name service service-name agent-specifier aci circuit-id-string ari remote-id-string] hierarchy level, you cannot also include the `static-interface` statement at this level. The `routing-instance` and `static-interface` statements are mutually exclusive for ACI/ARI pair configurations.

**Options**
- `routing-instance-name`—Name of the routing instance in which the router instantiates the dynamic PPPoE interface.

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

**Related Documentation**
- Configuring PPPoE Service Name Tables
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation
rpf-check (Dynamic Profiles)

Syntax

```
rpf-check {
   fail-filter filter-name;
   mode loose;
}
```

Hierarchy Level

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family]
```

Release Information


Description

Reduce forwarding of IP packets that might be spoofing and address by checking whether traffic is arriving on an expected path that the sender would use to reach the destination. You can include this statement with the `inet` protocol family only. When the traffic passes the check, it is forwarded to the destination address; otherwise it is discarded. When you configure `rpf-check` alone, then unicast RPF is in strict mode, meaning that the check passes only when the packet’s source address is in the FIB and the interface matches the routes RPF.

Starting in Junos OS Release 19.1, the `show interfaces statistics logical-interface-name detail` command displays unicast RPF statistics for dynamic logical interfaces when either `rpf-check` or `rpf-check mode loose` is enabled on the interface. No additional statistics are displayed when `rpf-check fail-filter filter-name` is configured on the interface. The `clear interfaces statistics logical-interface-name` command clears RPF statistics.

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

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

Related Documentation

- Unicast RPF in Dynamic Profiles for Subscriber Interfaces
- Configuring Unicast RPF Strict Mode on page 229
### rpf-check

#### List of Syntax

**Syntax (MX Series, SRX Series, M Series, T Series, PTX Series)** on page 968

**Syntax (EX Series and QFX Series)** on page 968

```plaintext
rpf-check {
    fail-filter filter-name;
    mode loose;
}
```

**Syntax (EX Series and QFX Series)**

```plaintext
rpf-check;
```

#### Hierarchy Level (MX Series, SRX Series, M Series, T Series, PTX Series)

- [edit interfaces interface-name unit logical-unit-number family inet]
- [edit interfaces interface-name unit logical-unit-number family inet6]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6]

#### Hierarchy Level (EX Series and QFX Series)

- [edit interfaces interface-name unit logical-unit-number family inet]
- [edit interfaces interface-name unit logical-unit-number family inet6]

#### Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Support for interface ps0 (pseudowire subscriber logical interface device) added in Junos OS Release 15.1.

#### Description

Enable a reverse-path forwarding (RPF) check on unicast traffic.

On EX3200 and EX4200 switches, enable a reverse-path forwarding (RPF) check on unicast traffic (except ECMP packets) on all ingress interfaces.

On EX4300 switches, enable a reverse-path forwarding (RPF) check on unicast traffic, including ECMP packets, on all ingress interfaces.

On EX8200 and EX6200 switches, enable an RPF check on unicast traffic, including ECMP packets, on the selected ingress interfaces.

On QFX Series switches, enable an RPF check on unicast traffic on the selected ingress interfaces. ECMP packets are checked by QFX5000 Series switches only.

The mode statement is explained separately.

#### Default

Unicast RPF is disabled on all interfaces.
Options  fail-filter—A filter to evaluate when packets are received on the interface. If the RPF check fails, this optional filter is evaluated. If the fail filter is not configured, the default action is to silently discard the packet.

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

Related Documentation
• Configuring Unicast RPF Strict Mode on page 229
• Configuring Unicast RPF Loose Mode on page 231
• Configuring a Pseudowire Subscriber Logical Interface Device
• Example: Configuring Unicast RPF (On a Switch)

rpf-loose-mode-discard

Syntax  rpf-loose-mode-discard {
        family {
            inet;
            inet6;
        }
    }

Hierarchy Level  [edit forwarding-options]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure unicast reverse path forwarding (unicast RPF) loose mode with the ability to discard packets with the source address pointing to the discard next hop.

Options  inet—IPv4 address family.
        inet6—IPv6 address family.

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

Related Documentation
• Understanding Unicast RPF (Routers) on page 226
rtp

Syntax

rtp {
  f-max-period number;
  queues [queue-numbers ];
  port {
    minimum port-number;
    maximum port-number;
  }
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number compression]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the real-time transport protocol (RTP) properties for voice services traffic.

The remaining statements are described separately.

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

• Junos OS Services Interfaces Library for Routing Devices
rts

Syntax  
rts (assert | de-assert | normal);

Hierarchy Level  
[edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For EIA-530 and V.35 interfaces only, configure the to-DCE signal, request to send (RTS).

Options  
assert—The to-DCE signal must be asserted.

de-assert—The to-DCE signal must be deasserted.

normal—Normal RTS signal handling, as defined by the TIA/EIA Standard 530.
Default: normal

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

Related Documentation  
• Configuring the Serial Signal Handling on page 324
rts-polarity

Syntax

rts-polarity (negative | positive);

Hierarchy Level

[edit interfaces interface-name serial-options]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure RTS signal polarity.

Options

negative—Negative signal polarity.
positive—Positive signal polarity.

Default: positive

Required Privilege

Level

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

Related Documentation

• Configuring Serial Signal Polarities on page 327
rtvbr

Syntax  

rtvbr peak rate sustained rate burst length;

Hierarchy Level  

[edit interfaces interface-name atm-options vpi vpi-identifier shaping ],  
[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ],  
[edit interfaces interface-name unit logical-unit-number shaping ],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number shaping ],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ]

Release Information  

Statement introduced before Junos OS Release 7.4.

Description  

For ATM2 IQ PICs only, define the real-time variable bandwidth utilization in the traffic-shaping profile.

When you configure the real-time bandwidth utilization, you must specify all three options (burst, peak, and sustained). You can specify the rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify the rate in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps.

Default  

If the rtvbr statement is not included, bandwidth utilization is unlimited.

Options  

burst length—Burst length, in cells. If you set the length to 1, the peak traffic rate is used.  

Range: 1 through 4000 cells

peak rate—Peak rate, in bits per second or cells per second.  

Range: For ATM2 IQ OC3 and OC12 interfaces, 33 Kbps through 542,526,792 bps. For ATM2 IQ OC48 interfaces, 33 Kbps through 2,170,107,168 bps. For ATM2 IQ DS3 and E3 interfaces, 33 Kbps through the maximum rate, which depends on the ATM encapsulation and framing you configure.

sustained rate—Sustained rate, in bps or cps.  

Range: For ATM2 IQ OC3 and OC12 interfaces, 33 Kbps through 542,526,792 bps. For ATM2 IQ OC48 interfaces, 33 Kbps through 2,170,107,168 bps. For ATM2 IQ DS3 and E3 interfaces, from 33 Kbps through the maximum rate, which depends on the ATM encapsulation and framing you configure.

Required Privilege Level  

interface—to view this statement in the configuration.  

interface-control—to add this statement to the configuration.
Related Documentation
- Configuring ATM CBR
- Configuring ATM2 IQ Real-Time VBR
- Applying Scheduler Maps to Logical ATM Interfaces
- cbr on page 465
- vbr on page 1113
sa-multicast (100-Gigabit Ethernet)

Syntax

```
sa-multicast;
```

Hierarchy Level

```
[edit chassis fpc slot pic slot forwarding-mode]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Configure the 100-Gigabit Ethernet PIC or MIC to interoperate with other Juniper Networks 100-Gigabit Ethernet PICs.

NOTE: The default packet steering mode for PD-1CE-CFP-FPC4 is SA multicast bit mode. No SA multicast configuration is required to enable this mode.

sa-multicast supports interoperability between the following PICs and MICs:

- 100-Gigabit Ethernet Type 5 PIC with CFP (PF-1CGE-CFP) and the 100-Gigabit Ethernet Type 4 PIC with CFP (PD-1CE-CFP-FPC4).
- 100-Gigabit Ethernet MICs and the 100-Gigabit Ethernet Type 4 PIC with CFP (PD-1CE-CFP-FPC4).

Required Privilege

Level

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

Related Documentation

- Interoperability Between the 100-Gigabit Ethernet PICs PD-1CE-CFP-FPC4 and PF-1CGE-CFP
- Configuring the Interoperability Between the 100-Gigabit Ethernet PICs PF-1CGE-CFP and PD-1CE-CFP-FPC4
- Configuring 100-Gigabit Ethernet MICs to Interoperate with Type 4 100-Gigabit Ethernet PICs (PD-1CE-CFP-FPC4) Using SA Multicast Mode
- Interoperability Between MPC4E (MPC4E-3D-2CGE-8XGE) and 100-Gigabit Ethernet PICs on Type 4 FPC
- Configuring MPC4E (MPC4E-3D-2CGE-8XGE) to Interoperate with 100-Gigabit Ethernet PICs on Type 4 FPC Using SA Multicast Mode
- Interoperability Between the 100-Gigabit Ethernet PICs PD-1CE-CFP-FPC4 and P1-PTX-2-100GE-CFP
- Configuring the Interoperability Between the 100-Gigabit Ethernet PICs P1-PTX-2-100GE-CFP and PD-1CE-CFP-FPC4
• forwarding-mode (100-Gigabit Ethernet)
• sa-multicast (PTX Series Packet Transport Routers)
• vlan-steering (100-Gigabit Ethernet Type 4 PIC with CFP) on page 1130
• Configuring VLAN Steering Mode for 100-Gigabit Ethernet Type 4 PIC with CFP

sampling (Interfaces)

Syntax    sampling direction;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the direction of traffic to be sampled.

Options direction can be one of the following:

input—Configure at least one expected ingress point.

output—Configure at least one expected egress point.

input output—On a single interface, configure at least one expected ingress point and one expected egress point.

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

Related Documentation
• Junos OS Services Interfaces Library for Routing Devices
• Configuring Flow Monitoring on T Series and M Series Routers and EX9200 Switches
satop-options

Syntax

satop-options {
  excessive-packet-loss-rate {
    apply-groups group-name
    apply-groups-except group-name
    groups group-name
    sample-period milliseconds
    threshold percentile
  }
  idle-pattern pattern
  jitter-buffer-auto-adjust
  jitter-buffer-latency milliseconds
  jitter-buffer-packets packets
  payload-size bytes;
}

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description
Set Structure-Agnostic TDM over Packet (SAtOP) protocol options.

On ACX Series routers, the following statements are not supported:

  apply-groups group-name
  apply-groups-except group-name
  groups group-name
  jitter-buffer-auto-adjust

Options
excessive-packet-loss-rate options—Set packet loss options.

- apply-groups group-name—Groups from which to inherit configuration data.
- apply-groups-except group-name—Don’t inherit configuration data from these groups.
- groups group-name—Specify groups.
- sample-period milliseconds—Number of milliseconds over which excessive packet loss rate is calculated.
- threshold percentile—Percentile designating the threshold of excessive packet loss rate (from 1 to 100).
- idle-pattern pattern—An 8–bit hexadecimal pattern to replace TDM data in a lost packet (from 0 to 255).
- jitter-buffer-auto-adjust—Automatically adjust the jitter buffer.
NOTE: This option is not applicable on MX Series routers.

jitter-buffer-latency milliseconds—Number of milliseconds delay in jitter buffer (from 1 to 1000 milliseconds).

jitter-buffer-packets packets—Number of packets in jitter buffer (from 1 to 64).

payload-size bytes—Payload size in integer number of bytes.

shared-interface

Syntax shared-interface;

Hierarchy Level [edit interfaces ge-fpc/pic/slot],
[edit interfaces so-fpc/pic/slot],
[edit interfaces xe-fpc/pic/slot]

Release Information Statement introduced in Junos OS Release 9.3.

Description Configure a physical interface to be a shared interface. Logical interfaces configured under the shared physical interface can be assigned to different Protected System Domains (PSDs).

Options This statement has no options.

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

Related Documentation • interface-shared-with on page 697
scheduler-maps (For ATM2 IQ Interfaces)

Syntax

```
scheduler-maps map-name {
    forwarding-class (class-name | assured-forwarding | best-effort | expedited-forwarding | network-control):
    vc-cos-mode (alternate | strict);
}
```

Hierarchy Level

```
[edit at-fpc/pic/port interface-name atm-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For ATM2 IQ interfaces only, define CoS parameters assigned to forwarding classes.

Options

`map-name`—Name of the scheduler map.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

- ATM2 IQ VC Tunnel CoS Components Overview
- Applying Scheduler Maps to ATM Interfaces
- `atm-scheduler-map` on page 431
**schedulers**

**Syntax**

`schedulers number;`

**Hierarchy Level**

`[edit interfaces interface-name]`

**Release Information**

Statement introduced in Junos OS Release 8.2.

**Description**

Specify the number of schedulers for Ethernet IQ2 and IQ2-E PIC port interfaces.

**Default**

If you omit this statement, the 1024 schedulers are distributed equally over all ports in multiples of 4.

**Options**

`number`—Number of schedulers to configure on the port.

**Range:** 1 through 1024

**Required Privilege Level**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

**Related Documentation**

- *Class of Service Feature Guide (Routers and EX9200 Switches)*

---

**secondary**

**Syntax**

`secondary interface-name;`

**Hierarchy Level**

`[edit interfaces (rsp0 | rsp1) redundancy-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Specify the secondary (backup) AS PIC interface or MultiServices PIC interface.

**Options**

`interface-name`—The identifier for the AS PIC interface or MultiServices PIC interface, which must be of the form `sp-fpc/pic/port`.

**Required Privilege Level**

`interface`—To view this statement in the configuration.

`interface-control`—To add this statement to the configuration.

**Related Documentation**

- *Junos OS Services Interfaces Library for Routing Devices*
send-critical-event

Syntax
send-critical-event;

Hierarchy Level
[edit protocols oam ethernet link-fault-management action-profile action]

Release Information
Statement introduced in Junos OS Release 8.5.

Description
Send OAM PDUs with the critical event bit set.

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

Related Documentation
• Specifying the Actions to Be Taken for Link-Fault Management Events
serial-options

Syntax serial-options {
    clock-rate rate;
    clocking-mode (dce | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    dsr-polarity (negative | positive);
    dte-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (negative | positive);
    encoding (nrz | nrzi);
    indication-polarity (negative | positive);
    line-protocol protocol;
    loopback (dce-local | dce-remote | local | remote);
    rts-polarity (negative | positive);
    tm-polarity (negative | positive);
    transmit-clock invert;
}

Hierarchy Level [edit interfaces se-pim/0/port]

Release Information Statement introduced prior to Junos OS Release 7.4.

Description Configure serial-specific interface properties.

The remaining statements are explained separately. See CLI Explorer.
server

Syntax server;

Hierarchy Level [edit interfaces pp0 unit logical-unit-number pppoe-options],
[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number pppoe-options]

Release Information Statement introduced in Junos OS Release 8.5.

Description Configure the router to operate in the PPPoE server mode. Supported on M120 and M320 Multiservice Edge Routers and MX Series 5G Universal Routing Platforms operating as access concentrators.

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

Related Documentation • Configuring the PPPoE Server Mode
server-timeout

Syntax  server-timeout seconds;

Hierarchy Level  [edit protocols dot1x authenticator interface interface-id]

Release Information  Statement introduced in Junos OS Release 9.3.

Description  Sets the number of seconds the port waits 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—The number of seconds the port waits for a response when relaying a request from the authentication server to the client before resending the request.

Range:  1 through 60 seconds
Default:  30 seconds

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

Related Documentation  • IEEE 802.1x Port-Based Network Access Control Overview
  • authenticator on page 434
  • dot1x on page 534
  • interface (IEEE 802.1x) on page 687
service (Logical Interfaces)

**Syntax**

```plaintext
service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
```

**Hierarchy Level**

- `[edit interfaces interface-name unit logical-unit-number family inet]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Define one or more service sets and filters, and one postservice filter to be applied to an interface.

**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**

- Junos OS Services Interfaces Library for Routing Devices
service (PPPoE)

Syntax

```
service service-name {
    drop;
    delay seconds;
    terminate;
    dynamic-profile profile-name;
    routing-instance routing-instance-name;
    max-sessions number;
    agent-specifier {
        aci circuit-id-string ari remote-id-string {
            drop;
            delay seconds;
            terminate;
            dynamic-profile profile-name;
            routing-instance routing-instance-name;
            static-interface interface-name;
        }
    }
}
```

Hierarchy Level

[edit protocols pppoe service-name-tables table-name]

Release Information

Statement introduced in Junos OS Release 10.0.

any, dynamic-profile, routing-instance, max-sessions, and static-interface options introduced in Junos OS Release 10.2.

Description

Specify the action taken by the interface on receipt of a PPPoE Active Discovery Initiation (PADI) control packet for the specified named service, empty service, or any service in a PPPoE service name table. You can also specify the dynamic profile and routing instance that the router uses to instantiate a dynamic PPPoE interface, and the maximum number of active PPPoE sessions that the router can establish with the specified service.

Default

The default action is terminate.

Options

- **service-name**—Service entry in the PPPoE service name table:
  - **service-name**—Named service entry of up to 32 characters; for example, premiumService. You can configure a maximum of 512 named service entries across all PPPoE service name tables on the router.
  - **empty**—Service entry of zero length that represents an unspecified service. Each PPPoE service name table includes one empty service entry by default.
  - **any**—Default service for non-empty service entries that do not match the named or empty service entries configured in the PPPoE service name table. Each PPPoE service name table includes one any service entry by default.
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**
- Configuring PPPoE Service Name Tables
- Assigning a Service to a Service Name Table and Configuring the Action Taken When the Client Request Includes a Non-zero Service Name Tag
- Configuring the Action Taken When the Client Request Includes an Empty Service Name Tag
- Configuring the Action Taken for the Any Service

### service-domain

**Syntax**
service-domain (inside | outside);

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

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For adaptive services interfaces, specify a service interface domain. If you specify this interface using the next-hop-service statement at the [edit services service-set service-set-name] hierarchy level, the interface domain must match that used with the inside-service-interface and outside-service-interface statements.

**Options**
- inside—Interface used within the network.
- outside—Interface used outside the network.

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

**Related Documentation**
- Junos OS Services Interfaces Library for Routing Devices
service-filter (Interfaces)

Syntax

```
service-filter filter-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet service (input | output) service-set service-set-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service (input | output) service-set service-set-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the filter to be applied to traffic before it is accepted for service processing. Configuration of a service filter is optional; if you include the `service-set` statement without a `service-filter` definition, Junos OS assumes the match condition is true and selects the service set for processing automatically.

Options

`filter-name`—Identifies the filter to be applied in service processing. You can include special characters, such as a forward slash (/), colon (:), or a period (.).

Required Privilege

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

Related Documentation

- *Applying Filters and Services to Interfaces*
- *Junos OS Services Interfaces Library for Routing Devices*
service-name-table

Syntax

```
service-name-table table-name;
```

Hierarchy Level

- [edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family pppoe],
- [edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family pppoe],
- [edit interfaces interface-name unit logical-unit-number family pppoe],
- [edit interfaces interface-name unit logical-unit-number family pppoe-underlying-options],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family pppoe],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number pppoe-underlying-options]

Release Information

Statement introduced in Junos OS Release 10.0.
Support at the [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.

Description

Specify the PPPoE service name table assigned to a PPPoE underlying interface. This underlying interface is configured with either the `encapsulation ppp-over-ether` statement or the `family pppoe` statement; the two statements are mutually exclusive.

NOTE: The [edit ... family pppoe] hierarchies are supported only on MX Series routers with MPCs.

Options

- `table-name`—Name of the PPPoE service name table, a string of up to 32 alphanumeric characters.

Required Privilege

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

Related Documentation

- Configuring PPPoE Service Name Tables
- Assigning a Service Name Table to a PPPoE Underlying Interface
- Configuring the PPPoE Family for an Underlying Interface
**service-name-tables**

**Syntax**

```
service-name-tables table-name {
  service service-name {
    drop;
    delay seconds;
    terminate;
    dynamic-profile profile-name;
    routing-instance routing-instance-name;
    max-sessions number;
    agent-specifier {
      acl circuit-id-string ari remote-id-string {
        drop;
        delay seconds;
        terminate;
        dynamic-profile profile-name;
        routing-instance routing-instance-name;
        static-interface interface-name;
      }
    }
  }
}
```

**Hierarchy Level**

[edit protocols pppoe]

**Release Information**


**Description**

Create and configure a PPPoE service name table. Specify the action taken for each service and remote access concentrator on receipt of a PPPoE Active Discovery Initiation (PADI) packet. You can also specify the dynamic profile and routing instance that the router uses to instantiate a dynamic PPPoE interface, and the maximum number of active PPPoE sessions that the router can establish with the specified service. A maximum of 32 PPPoE service name tables is supported per router.

**Options**

**table-name**—Name of the PPPoE service name table, a string of up to 32 alphanumeric characters.

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**

- Configuring PPPoE Service Name Tables
- Creating a Service Name Table
service-set

Syntax  
```
service-set service-set-name;
```

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number family inet service (input | output) service-set service-set-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service (input | output) service-set service-set-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define one or more service sets to be applied to an interface. If you define multiple service sets, the Junos OS evaluates the filters in the order in which they appear in the configuration.

Options
```
service-set-name—Identifies the service set.
```

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

Related Documentation
- Junos OS Services Interfaces Library for Routing Devices
services (Priority Level)

Syntax
services priority-level;

Hierarchy Level
[edit interfaces interface-name services-options sysloghost hostname]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify system logging priority level.

Options
priority-level—Assigns a priority level to the facility. Valid entries are as follows:

- alert—Conditions that should be corrected immediately.
- any—Matches any level.
- emergency—Panic conditions.
- critical—Critical conditions.
- error—Error conditions.
- info—Informational messages.
- notice—Conditions that require special handling.
- warning—Warning messages.

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

Related Documentation
- Junos OS Services Interfaces Library for Routing Devices
services-options

Syntax

services-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    session-limit {
        maximum number;
        rate new-sessions-per-second;
    }
    syslog {
        host hostname {
            facility-override facility-name;
            log-prefix prefix-number;
            services priority-level;
        }
    }
}

Hierarchy Level

[edit interfaces interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the service options to be applied on an interface.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

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

Related Documentation

• Junos OS Services Interfaces Library for Routing Devices
**shaping**

Syntax

```plaintext
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
  queue-length number;
}
```

Hierarchy Level

- [edit interfaces interface-name atm-options vpi vpi-identifier]
- [edit interfaces interface-name unit logical-unit-number]
- [edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For ATM encapsulation only, define the traffic-shaping profile.

For Circuit Emulation PICs, specify traffic shaping in the ingress and egress directions.

For ATM2 IQ interfaces, changing or deleting VP tunnel traffic shaping causes all logical interfaces on a VP to be deleted and then re-added.

VP tunnels are not supported on multipoint interfaces.

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

- Defining Virtual Path Tunnels
- Defining the ATM Traffic-Shaping Profile Overview
- Configuring ATM QoS or Shaping
- Applying Scheduler Maps to Logical ATM Interfaces
shdsl-options

Syntax

shdsl-options {
    annex (annex-a | annex-b);
    line-rate line-rate;
    loopback (local | remote | payload);
    snr-margin {
        snext margin;
    }
}

Hierarchy Level

[edit interfaces interface-name],
[edit logical-systems logical-system-name interfaces interface-name]

Release Information
Statement introduced in Junos OS Release 7.4.

Description
For J Series Services Routers only, configure symmetric DSL (SHDSL) options.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
short-name-format

Syntax  short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);

Hierarchy Level [edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

Description Specify the name format of the maintenance association name.

Options character-string—The name is an ASCII character string.
   vlan—The primary VLAN identifier.
   2octet—A number in the range 0 through 65,535.
   rfc-2685-vpn-id—A VPN identifier that complies with RFC 2685.
Default: character-string

NOTE: The PTX Series Packet Transport Routers support the vlan and 2octet options only.

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

Related Documentation • Creating a Maintenance Association
**short-sequence**

**Syntax**  
short-sequence;

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

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For multilink interfaces only, set the length of the packet sequence identification number to 12 bits.

**Default**  
If you omit this statement from the configuration, the length is set to 24 bits.

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

**Related Documentation**  
• *Junos OS Services Interfaces Library for Routing Devices*
sla-iterator-profile

Syntax

```
sla-iterator-profile profile-name {
  data-tlv-size size;
  iteration-count count-value;
  priority priority-value;
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
```

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Configure a remote MEP with an iterator profile and specify the options.

Y.1731 performance monitoring (PM) over Aggregated Ethernet Interfaces is not supported on EX4300 switches.

Options

```
profile-name—Name of the iterator profile configured for a remote MEP. For more information about configuring a remote MEP with an iterator profile, see Configuring a Remote MEP with an Iterator Profile.
```

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation

- Configuring an Iterator Profile
- Configuring a Remote MEP with an Iterator Profile
- Verifying the Configuration of an Iterator Profile
- Managing Iterator Statistics
- sla-iterator-profiles on page 999
sla-iterator-profiles

Syntax
sla-iterator-profiles {
    profile-name {
        avg-fd-twoway-threshold;
        avg-ifdv-twoway-threshold;
        avg-flr-forward-threshold;
        avg-flr-backward-threshold;
        calculation-weight {
            delay delay-weight;
            delay-variation delay-variation-weight;
        }
        cycle-time milliseconds;
        flap-trap-monitor seconds
        iteration-period iteration-period-value;
        measurement-type (loss | statistical-frame-loss | two-way-delay);
    }
}

Hierarchy Level  [edit protocols oam ethernet connectivity-fault-management performance-monitoring]


Description  Configure an iterator application and specify the iterator profile options.

Options  profile-name—Name of the iterator profile. For more information about configuring the iterator profile, see Configuring an Iterator Profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level  Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation  • Configuring an Iterator Profile
• Configuring a Remote MEP with an Iterator Profile
• Verifying the Configuration of an Iterator Profile
• Managing Iterator Statistics
**snr-margin**

**Syntax**
```
snr-margin {
    snext margin;
}
```

**Hierarchy Level**
- [edit interfaces interface-name shdsl-options],
- [edit logical-systems logical-system-name interfaces interface-name shdsl-options]

**Release Information**
Statement introduced in Junos OS Release 7.4.

**Description**
For J Series Services Routers only, configure the SHDSL signal-to-noise ratio (SNR) margin. The SNR margin is the difference between the desired SNR and the actual SNR. Configuring the SNR creates a more stable SHDSL connection by making the line train at a SNR margin higher than the threshold. If any external noise below the threshold is applied to the line, the line remains stable.

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**
- [Junos OS Interfaces and Routing Configuration Guide](#)
**snex**

**Syntax**

```
Syntax     snext margin;
```

**Hierarchy Level**

```
HierarchyLevel [edit interfaces interface-name shdsl-options snr-margin],
                [edit logical-systems logical-system-name interfaces interface-name shdsl-options
                 snr-margin]
```

**Release Information**

Statement introduced in Junos OS Release 7.4.

**Description**

For J Series Services Routers only, configure self-near-end crosstalk (SNEXT) signal-to-noise ratio (SNR) margin for a SHDSL line. When configured, the line trains at higher than SNEXT threshold. The SNR margin is the difference between the desired SNR and the actual SNR.

**Options**

```
Options    margin—Desired SNEXT margin. Possible values are disabled or a margin between –10dB
           and 10 dB.
           Default: disabled
```

**Required Privilege**

```
Required Privilege interface—to view this statement in the configuration.
Level      interface-control—to add this statement to the configuration.
```

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide
sonet-options

Syntax

sonet-options {
    aps {
        advertise-interval milliseconds;
        annex-b
        authentication-key key;
        (break-before-make | no-break-before-make);
        fast-aps-switch;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        switching-mode (bidirectional | unidirectional);
        working-circuit group-name;
    }
    bytes {
        c2 value;
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (16 | 32);
    loopback (local | remote);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
    rfc-2615;
    trigger {
        defect ignore;
        defect hold-time up milliseconds down milliseconds;
    }
}

vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.
**Description** Configure SONET/SDH-specific interface properties.

On SONET/SDH OC48 interfaces that you configure for channelized (multiplexed) mode (by including the `no-concatenate` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level), the `bytes el-quiet` and `bytes f1` options have no effect. The `bytes f2, bytes z3, bytes z4`, and `path-trace` options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

On a channelized OC12 interface, the `bytes el-quiet, bytes f1, bytes f2, bytes z3, and bytes z4` options are not supported. The `fcs` and `payload-scrambler` statements are also not supported; you must configure these for each DS3 channel using the `t3-options fcs` and `t3-options payload-scrambler` statements. The `aps` and `loopback` statements are supported only on channel 0 and are ignored if included in the configurations for channels 1 through 11. You can configure loopbacks for each DS3 channel with the `t3-options loopback` statement. The `path-trace` statement can be included in the configuration for each DS3 channel, thereby configuring a unique path trace for each channel.

To configure loopback on channelized IQ and IQE PICs, SONET/SDH level, use the `loopback` statement `local` and `remote` options at the controller interface (`coc48, cstm16, coc12, cstm4, coc3, and cstm1`). It is ignored for path-level interfaces `so-fpc/pic/port` or `so-fpc/pic/port:channel`.

If you are running Intermediate System-to-Intermediate System (IS-IS) over SONET/SDH interfaces, use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run HDLC, configure an ISO family MTU of 4469 on the router.

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 SONET/SDH Parameters on ATM Interfaces
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
- Channelized STMI Interfaces Overview
- SONET/SDH Interfaces Overview
- `no-concatenate`
source

Syntax  

source source-address;

Hierarchy Level (EX, NFX, OCX1100 and QFX Series)  

[edit interfaces interface-name unit logical-unit-number tunnel]

Hierarchy Level (M-series and T-series)  

[edit interfaces interface-name unit logical-unit-number tunnel address], 
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number tunnel address]

Release Information

Statement introduced before Junos OS Release 7.4. 
Statement introduced in Junos OS Release 12.1 for EX Series switches. 
Statement introduced in Junos OS Release 13.2 for the QFX Series. 
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Specify the source address of the tunnel.

Default

If you do not specify a source address, the tunnel uses the unit’s primary address as the source address of the tunnel.

Options

source-address—Address of the local side of the tunnel. This is the address that is placed in the outer IP header’s source field.

Required Privilege Level

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

Related Documentation

• Tunnel Services Overview
• multicast-only on page 803
• primary (Address on Interface) on page 922
• Junos OS Services Interfaces Library for Routing Devices
**source-address-filter**

**Syntax**

```
source-address-filter {
    mac-address;
}
```

**Hierarchy Level**

```
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.

**Description**

For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, Gigabit Ethernet IQ interfaces, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), specify the MAC addresses from which the interface can receive packets. For this statement to have any effect, you must include the source-filtering statement in the configuration to enable source address filtering.

**Options**

- **mac-address**—MAC address filter. You can specify the MAC address as `nn:nn:nn:nn:nn:nn` or `nnnn.nnnn.nnnn`, where `n` is a decimal digit. To specify more than one address, include multiple `mac-address` options in the source-address-filter statement.

If you enable the VRRP on a Fast Ethernet or Gigabit Ethernet interface, as described in VRRP and VRRP for IPv6 Overview, and if you enable MAC source address filtering on the interface, you must include the virtual MAC address in the list of source MAC addresses that you specify in the source-address-filter statement. MAC addresses ranging from `00:00:5e:00:01:00` through `00:00:5e:01:00` are reserved for VRRP, as defined in RFC 3768, Virtual Router Redundancy Protocol. When you configure the VRRP group, the group number must be the decimal equivalent of the last hexadecimal byte of the virtual MAC address.

On untagged Gigabit Ethernet interfaces, you should not configure the source-address-filter statement and the accept-source-mac statement simultaneously. On tagged Gigabit Ethernet interfaces, you should not configure the source-address-filter statement and the accept-source-mac statement with an identical MAC address specified in both filters.

**Required Privilege Level**

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

**Related Documentation**

- Configuring MAC Address Filtering for Ethernet Interfaces
- Configuring MAC Address Filtering on PTX Series Packet Transport Routers
- source-filtering on page 841
**source-class-usage**

**Syntax**

```plaintext
source-class-usage [ 
    direction; 
]
```

**Hierarchy Level**

- [edit interfaces interface-name unit logical-unit-number family inet accounting],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet accounting],
- [edit routing-instances routing-instance-name vrf-table-label]

**Release Information**


**Description**

Enable packet counters on an interface that count packets that arrive from specific prefixes on the provider core router and are destined for specific prefixes on the customer edge router.

**Options**

`direction` can be one of the following:

- `input`—Configure at least one expected ingress point.
- `output`—Configure at least one expected egress point.
- `input output`—On a single interface, configure at least one expected ingress point and one expected egress point.

**Required Privilege Level**

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

**Related Documentation**

- [Enabling Source Class and Destination Class Usage on page 241](#)
- [accounting on page 395](#)
- [destination-class-usage on page 521](#)
- [Junos OS Services Interfaces Library for Routing Devices](#)
- [vrf-table-label](#)
source-filtering

**Syntax**

(source-filtering | no-source-filtering);

**Hierarchy Level**

[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Packet Transport Routers.

**Description**

For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and Gigabit Ethernet IQ interfaces only, enable the filtering of MAC source addresses, which blocks all incoming packets to that interface. To allow the interface to receive packets from specific MAC addresses, include the `source-address-filter` statement.

If the remote Ethernet card is changed, the interface is no longer able to receive packets from the new card because it has a different MAC address.

**Default**

Source address filtering is disabled.

**Required Privilege Level**

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

**Related Documentation**

- Configuring MAC Address Filtering for Ethernet Interfaces
- Configuring MAC Address Filtering on PTX Series Packet Transport Routers
- accept-source-mac on page 391
- source-address-filter on page 1005
**speed (Ethernet)**

| Syntax (EX Series) | speed (auto-negotiation | speed) ; |
|--------------------|------------------------------------------------|
| Syntax (EX2300 and EX4300) | speed speed; |
| Syntax (EX Series, ACX Series, MX Series) | speed (10m | 10g | 100m | 1g | 2.5g | 5g | auto | auto-10m-100m); |
| Syntax (ACX5448) | speed (100m | 1g | auto); |
| Syntax (QFX Series, OCX1100, EX4600) | speed (10g | 1g | 100m) |
| Syntax (PTX10003-80C, PTX10003-160C) | speed (10g | 40g | 100g) |

Hierarchy Level (EX Series)

[edit interfaces interface-name ether-options]

Hierarchy Level (EX2300 and EX4300)

[edit interfaces interface-name]

Hierarchy Level (ACX5448)

[edit interfaces interface-name]

Hierarchy Level (ACX Series, EX Series, MX Series)

[edit interfaces interface-name],
[edit interfaces ge-pim/0/0 switch-options switch-port port-number]

Hierarchy Level (QFX Series, EX4600, OCX Series)

[edit interfaces 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 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Speed option 2.5Gbps introduced in Junos OS Release 18.1R2 for EX2300 switch.
Speed option 10Gbps and 5Gbps introduced in Junos OS Release 18.2R1 for EX4300 switch.
Speed option 1-Gbps is introduced in Junos OS Release 19.1R1 on the 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module on EX4300-48MP switches.
Speed options 100-Mbps, 1-Gbps, and auto is introduced in Junos OS Releases 18.4R1S2, 18.4R2, and 19.2R1 and later for ACX5448 Universal Metro Routers.
Speed option 10Gbps, 40Gbps, and 100Gbps introduced in Junos OS Evolved Release 19.1R1 for PTX10003-80C, PTX10003-160C routers.
Configure the interface speed. This statement applies to the management Ethernet interface (fxp0 or em0), Fast Ethernet 12-port and 48-port PICs, the built-in Fast Ethernet port on the FIC (M7 router), Combo Line Rate DPCs and Tri-Rate Ethernet Copper interfaces on MX Series routers, and Gigabit Ethernet interfaces on EX Series switches.

When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled. When you configure 100BASE-FX SFP, you must set the port speed at 100 Mbps.

NOTE: On MX Series routers with Tri-rate Enhanced DPC (DPCE-R-40GE-TX), when you configure the interface speed using the auto-10m-100m option, the speed is negotiated to the highest value possible (100 Mbps), if the same value is configured on both sides of the link. However, when you view the interface speed of the DPC, using the show interfaces command, the value of the speed is not accurately displayed. For instance, if you configure the speed of the Tri-rate enhanced DPC, as 100Mbps on both sides of the link, the interface speed of the DPC is negotiated to 100 Mbps. However, the interface speed of the DPC displays 1 bps. This is an issue with the show interfaces command only. The actual interface speed is 100 Mbps.

On 10-Gigabit Ethernet SFP interfaces, autonegotiation is enabled by default and auto-detects the speed to be either 1 Gbps or 10 Gbps. On QFX5100-48S, QFX5100-96S, and QFX5100-24Q devices using 10-Gigabit Ethernet SFP interfaces, the speed is set to 10 Gbps by default and cannot be configured to operate in a different speed. On QFX5100-48S and QFX5100-96S devices using 1-Gigabit Ethernet SFP interfaces, the speed is set to 1 Gbps by default and cannot be configured to operate in a different speed.

NOTE: In Junos OS Release 14.1X53-D35 on QFX5100-48T-6Q devices using 10-Gigabit Ethernet Copper interfaces, autonegotiation is disabled by default on the copper ports, and the interfaces operate at a speed of 100M. You can, however, enable auto-negotiation by issuing the set interface name ether-options auto-negotiation command on the interface for which you want to change the interface speed. With autonegotiation enabled, the interface auto-detects the speed in which to operate.

NOTE: Only 10 Gbps and 40 Gbps interfaces are supported on OCX Series switches.

NOTE: When displaying interface information with show interfaces commands, you might see speed values for 1 Gbps interfaces displayed as 1000mbps.
(For EX2300 only) Starting in Junos OS Release 18.1R2, the multi-rate speed is supported on EX2300-48MP and EX2300-24MP switches. The speed configuration statement is supported on both multi-rate gigabit ethernet interface (mge) and gigabit ethernet (ge) interface. The mge interface is a rate-selectable (multirate) Gigabit Ethernet interface that can support speeds of 10-Gbps, 5-Gbps, and 2.5-Gbps over CAT5e/CAT6/CAT6a cables. In the EX2300, the mge interface supports 100-Mbps, 1-Gbps, and 2.5-Gbps speeds, which can be configured by using the speed configuration statement. Note that 10Mbpss speed is supported only on ge interfaces of EX2300 switch.

On EX2300-24MP and EX2300-48MP switches, if both Energy Efficient Ethernet (EEE) and 100-Mbps speed are configured on a rate-selectable (ormultirate) Gigabit Ethernet (mge) port, the port operates only at 100-Mbps speed but EEE is not enabled on that port. EEE is supported only on mge interfaces that operate at 1-Gbps and 2.5-Gbps speeds.

(For EX4300-48MP only) Starting with Junos OS Release 19.1R1, the 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module (EX-UM-4SFPP-MR) on EX4300-48MP switches supports 1-Gbps speed. You do not need to explicitly configure 1-Gbps speed on the uplink module as it automatically identifies the installed 1-gigabit SFP transceivers and creates the interface accordingly.

---

**NOTE:** On EX4300-48MP, the status LED of 1-Gigabit Ethernet uplink module port is solid green (instead of blinking green) because of a device limitation. However, there is no impact on device functionality.

---

(For ACX5448 only) 100-Mbps speed is supported from interfaces xe-0/0/24 to xe-0/0/47 only.

**Default (EX Series)** If the auto-negotiation statement at the [edit interfaces interface-name ether-options] hierarchy level is enabled, the auto-negotiation option is enabled by default.
Options

You can specify the speed as either 10m (10 Mbps), 100m (100 Mbps), and on MX Series routers, 1g (1 Gbps). You can also specify the auto option on MX Series routers.

For Gigabit Ethernet interfaces on EX Series switches, you can specify one of the following options:
### Table 27: Options for speed

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Speed Supported</th>
<th>Auto-negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX Series Switches</td>
<td>100m—100 Mbps</td>
<td>auto-negotiation—Automatically negotiate the speed based on the speed of the other end of the link. This option is available only when the <code>auto-negotiation</code> statement at the <code>edit interfaces interface-name ether-options</code> hierarchy level is enabled.</td>
</tr>
<tr>
<td></td>
<td>10m—10 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1g—1 Gbps</td>
<td></td>
</tr>
<tr>
<td>ACX, MX Series</td>
<td>100m—100 Mbps</td>
<td>auto—Automatically negotiate the speed (10 Mbps, 100 Mbps, or 1 Gbps) based on the speed of the other end of the link.</td>
</tr>
<tr>
<td></td>
<td>10m—10 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1g—1 Gbps</td>
<td></td>
</tr>
<tr>
<td>EX4600, QFX Series, QFabric, OCX100</td>
<td>10g—10 Gbps</td>
<td>auto-negotiation—Automatically negotiate the speed based on the speed of the other end of the link. This option is available only when the <code>auto-negotiation</code> statement at the <code>edit interfaces interface-name ether-options</code> hierarchy level is enabled.</td>
</tr>
<tr>
<td></td>
<td>1g—1 Gbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>100m—100 Mbps</td>
<td></td>
</tr>
<tr>
<td>PTX10003-80C, and PTX10003-160C</td>
<td>10g—10 Gbps</td>
<td>speed—Specify the interface speed. Use number-of-sub-ports configuration statement to configure the number of optical channels for a particular port if the optics are used in a channelized mode. You can use this configuration option to configure a speed (10, 40, and 100 Gbps) in different number of channels based on the optics used. See PTX10003 Router Rate-Selectability Overview for more details.</td>
</tr>
<tr>
<td></td>
<td>40g—40 Gbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>100g—100 Gbps</td>
<td></td>
</tr>
<tr>
<td>EX2300</td>
<td>10m—10 Mbps (supported on EX series switches and only on ge interfaces of EX2300 switch)</td>
<td>speed—Specify the interface speed. If the <code>auto-negotiation</code> statement at the <code>edit interfaces interface-name ether-options</code> hierarchy level is disabled, you must specify a specific value. This value sets the speed that is used on the link. If the <code>auto-negotiation</code> statement is enabled, you might want to configure a specific speed value to advertise the desired speed to the remote end. The Multi-rate gigabit ethernet interface (MGE) on EX2300-24MP and EX2300-48MP switches flaps (becomes unavailable, and then available again) while performing timeout detection and recovery (TDR) test.</td>
</tr>
<tr>
<td></td>
<td>100m—100 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1g—1 Gbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.5g—2.5 Gbps (supported only on mge interfaces of E2300 switch)</td>
<td></td>
</tr>
<tr>
<td>EX4300-48MP (EX-UM-4SFPP-MR)</td>
<td>10m—10 Mbps (supported only on ge interfaces)</td>
<td>speed—Specify the interface speed.</td>
</tr>
<tr>
<td></td>
<td>100m—100 Mbps (supported on ge and mge interfaces)</td>
<td>NOTE: On 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module, no explicit configuration is required as it automatically identifies the transceivers and creates the interface accordingly.</td>
</tr>
<tr>
<td></td>
<td>1g—1 Gbps (supported on ge, mge interfaces, and 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module on EX4300-48MP switches). The 1-Gbps speed is supported on the 4-port</td>
<td></td>
</tr>
</tbody>
</table>
Table 27: Options for speed (continued)

1-Gigabit Ethernet/10-Gigabit Ethernet uplink module of EX4300-48MP switches from Junos OS Release 19.1R1 onwards.

- **2.5g**—2.5 Gbps (supported only on mge interfaces)
- **5g**—5 Gbps (supported only on mge interfaces)
- **10g**—10 Gbps (supported on mge interfaces and 4-port 1-Gigabit Ethernet/10-Gigabit Ethernet uplink module on EX4300-48MP switches)

### Required Privilege Level

- **interface**—To view this statement in the configuration.
- **interface-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>18.2R1</td>
<td>Starting in Junos OS Release 18.1R2, the multi-rate speed is supported on EX2300-48MP and EX2300-24MP switches.</td>
</tr>
</tbody>
</table>

### Related Documentation

- [Configuring the Interface Speed on page 100](#)
- *Configuring the Interface Speed on Ethernet Interfaces*
- *Configuring Gigabit Ethernet Autonegotiation*
- *Configuring Gigabit Ethernet Interfaces for EX Series Switches with ELS support*
- *auto-negotiation*
- *Configuring Gigabit and 10-Gigabit Ethernet Interfaces for EX4600 and QFX Series Switches*
- *Junos OS Network Interfaces Library for Routing Devices*
- *Configuring Gigabit Ethernet Interfaces (CLI Procedure)*
- *Configuring Gigabit Ethernet Interfaces (J-Web Procedure)*
- *Junos OS Ethernet Interfaces Configuration Guide*
speed (MX Series DPC)

Syntax

speed (auto | 1Gbps | 100Mbps | 10Mbps);

Hierarchy Level

[edit interfaces ge-fpc/pic/port]

Release Information

Statement introduced in Junos OS Release 9.5.

Description

On MX Series routers with Combo Line Rate DPCs and Tri-Rate Copper SFPs you can set autonegotiation of speed. To specify the autonegotiation speed, use the speed (auto | 1Gbps | 100Mbps | 10Mbps) statement under the [edit interface ge-/fpc/pic/port] hierarchy level. The auto option will attempt to automatically match the rate of the connected interface. To set port speed negotiation to a specific rate, set the port speed to 1Gbps, 100Mbps, or 10Mbps.

NOTE: If the negotiated speed and the interface speed do not match, the link will not be brought up. Half duplex mode is not supported.

Options

You can specify the speed as either auto (autonegotiate), 10Mbps (10 Mbps), 100Mbps (100 Mbps), or 1Gbps (1 Gbps).

Required Privilege Level

interface—To view this statement in the configuration.

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

Related Documentation

• Configuring Gigabit Ethernet Autonegotiation

• no-auto-mdix on page 823
speed (SONET/SDH)

Syntax  speed (oc3 | oc12 | oc48);

Hierarchy Level  [edit interfaces so-fpc/pic/port],
                 [edit interfaces so-fpc/pic/port:channel]

Release Information  Statement introduced in Junos OS Release 8.3.

Description  Configure the interface speed. This statement applies to SONET/SDH interfaces on
             next-generation SONET/SDH Type 1 and Type 2 PICs with SFP. Available speeds depend
             on whether the PIC is in concatenated mode or nonconcatenated mode. Include the
             channel in the interface name when configuring nonconcatenated interfaces.

Options  oc3 | oc12 | oc48—Speed when the PIC is in concatenated mode. For example, you can
         configure each port of a 4-port OC12 PIC to have a speed of oc3.

         You can configure port 0 of a 4-port OC12 PIC to have a speed of oc12.

         oc3 | oc12—Speed when the PIC is in nonconcatenated mode.

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

Related Documentation  • Configuring SONET/SDH Interface Speed on page 104
### spid1

**Syntax**

`spid1 spid1-string;`

**Hierarchy Level**

`[edit interfaces br-pim/0/port isdn-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure the Service Profile Identifier (SPID).

**Options**

`spid1-string`—Numeric SPID.

**Required Privilege Level**

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

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide

### spid2

**Syntax**

`spid2 spid2-string;`

**Hierarchy Level**

`[edit interfaces br-pim/0/port isdn-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure an additional SPID.

**Options**

`spid2-string`—Numeric SPID.

**Required Privilege Level**

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

**Related Documentation**
stacked-vlan-ranges

Syntax

stacked-vlan-ranges {
  access-profile profile-name;
  authentication {
    packet-types [packet-types];
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      mac-address;
      option-18
      option-37
      option-62;
      radius-realm radius-realm-string;
      user-prefix user-prefix-string;
      vlan-tags;
    }
  }
  dynamic-profile profile-name {
    accept (any | dhcp-v4 | inet);
    access-profile vlan-dynamic-profile-name;
    ranges (any | low-tag–high-tag),(any | low-tag–high-tag);
  }
  override;
}

Hierarchy Level

[edit interfaces interface-name auto-configure]

Release Information

Statement introduced in Junos OS Release 9.5.

Description

Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.

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

- Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs
- Configuring Interfaces to Support Both Single and Stacked VLANs
stacked-vlan-tagging

Syntax

stacked-vlan-tagging;

Hierarchy Level

[edit interfaces interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description

For Gigabit Ethernet IQ interfaces, Gigabit Ethernet, 10-Gigabit Ethernet LAN/WAN PIC, and 100-Gigabit Ethernet Type 5 PIC with CFP, enable stacked VLAN tagging for all logical interfaces on the physical interface.

For pseudowire subscriber interfaces, enable stacked VLAN tagging for logical interfaces on the pseudowire service.

Required Privilege Level

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

Related Documentation

• Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview
**start-end-flag**

**Syntax**  
start-end-flag (filler | shared);

**Hierarchy Level**  
[edit interfaces e1-fpc/pic/port],  
[edit interfaces t1-fpc/pic/port],  
[edit interfaces interface-name ds0-options],  
[edit interfaces interface-name e1-options],  
[edit interfaces interface-name e3-options],  
[edit interfaces interface-name t1-options],  
[edit interfaces interface-name t3-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

**Description**  
For DS0, E1, E3, T1, and T3 interfaces, configure the interface to share the transmission of start and end flags.

**NOTE:** When configuring E1 or T1 interfaces on the 10-port Channelized E1/T1 IQE PIC, the start-end-flag statement must be included at the [edit interfaces e1-fpc/pic/port] or [edit interfaces t1-fpc/pic/port] hierarchy level as appropriate.

**Options**  
filler—Wait two idle cycles between the start and end flags.  
shared—Share the transmission of the start and end flags. This is the default.

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

**Related Documentation**  
• Configuring E1 Start and End Flags  
• Configuring the E3 Start and End Flags  
• Configuring T1 Start and End Flags  
• Configuring T3 Start and End Flags
### static-interface

**Syntax**

static-interface interface-name;

**Hierarchy Level**

[edit protocols pppoe service-name-tables table-name service service-name agent-specifier aci circuit-id-string ari remote-id-string]

**Release Information**

Statement introduced in Junos OS Release 10.2.

**Description**

Reserve the specified static PPPoE interface for use only by the PPPoE client with matching agent circuit identifier (ACI) and agent remote identifier (ARI) information. You can specify only one static interface per ACI/ARI pair configured for a named service entry, empty service entry, or any service entry in the PPPoE service name table.

The static interface associated with an ACI/ARI pair takes precedence over the general pool of static interfaces associated with the PPPoE underlying interface.

If you include the static-interface statement in the configuration, you cannot also include either the dynamic-profile statement or the routing-instance statement. The dynamic-profile, routing-instance, and static-interface statements are mutually exclusive for ACI/ARI pair configurations.

**Options**

interface-name—Name of the static PPPoE interface reserved for use by the PPPoE client with matching ACI/ARI information. Specify the interface in the format pp0.logical, where logical is a logical unit number from 0 through 16385 for static interfaces.

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Configuring PPPoE Service Name Tables
- Reserving a Static PPPoE Interface for Exclusive Use by a PPPoE Client
**static-tei-val**

**Syntax**

static-tei-val value;

**Hierarchy Level**

[edit interfaces br-pim/0/port isdn-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For J Series Services Routers only. Statically configure the Terminal Endpoint Identifier (TEI) value. The TEI value represents any ISDN-capable device attached to an ISDN network that is the terminal endpoint. TEIs are used to distinguish between several different devices using the same ISDN links.

**Options**

value—Value between 0 through 63.

**Required Privilege Level**

interface—To view this statement in the configuration.

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

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide
## supplicant

**Syntax**  
`supplicant single;`

**Hierarchy Level**  
`[edit protocols dot1x authenticator interface interface-id]`

**Release Information**  
Statement introduced in Junos OS Release 9.3.

**Description**  
Specify the supplicant mode. Only single mode is supported.

This option will authenticate only the first client that connects to a port. All other clients that connect later (802.1x compliant or non-compliant) will be 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.

**Options**  
- `single`—Sets single mode.

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

**Related Documentation**  
- *IEEE 802.1x Port-Based Network Access Control Overview*
- `authenticator` on page 434
- `dot1x` on page 534
- `interface (IEEE 802.1x)` on page 687
### supplicant-timeout

**Syntax**  
supplicant-timeout seconds;

**Hierarchy Level**  
[edit protocols dot1x authenticator interface interface-id]

**Release Information**  
Statement introduced in Junos OS Release 9.3.

**Description**  
Specify the number of seconds the port waits for a response when relaying a request from the authentication server to the client before resending the request.

**Options**  
- **seconds**—Specify the number of seconds the port waits for the supplicant timeout.  
  - **Range:** 1 through 60 seconds  
  - **Default:** 30 seconds

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

**Related Documentation**  
- [IEEE 802.1x Port-Based Network Access Control Overview](#)  
- authenticator on page 434  
- dot1x on page 534  
- interface (IEEE 802.1x) on page 687
swap

Syntax  swap;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number input-vlan-map],  
[edit interfaces interface-name unit logical-unit-number output-vlan-map],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],  
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Release Information  Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.  
Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

Description  Specify the VLAN rewrite operation to replace a VLAN tag. The outer VLAN tag of the frame is overwritten with the user-specified VLAN tag information.  

On MX Series routers, you can enter this statement on Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, aggregated Ethernet using Gigabit Ethernet IQ interfaces, and 100-Gigabit Ethernet Type 5 PIC with CFP. On EX Series switches, you can enter this statement on Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces.

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

Related Documentation  •  Rewriting the VLAN Tag on Tagged Frames  
•  Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
swap-push

Syntax

```
swap-push;
```

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]

Release Information

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the VLAN rewrite operation to replace the outer VLAN tag of the frame with a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.

You can use this statement on Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, and for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, and 100-Gigabit Ethernet Type 5 PIC with CFP.

Required Privilege

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

Related Documentation

- [Rewriting a VLAN Tag and Adding a New Tag](#)
**swap-swap**

**Syntax**  
```
swap-swap;
```

**Hierarchy Level**  
```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]
```

**Release Information**  
Statement introduced in Junos OS Release 8.1.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**  
Specify the VLAN rewrite operation to replace both the inner and the outer VLAN tags of the frame with a user-specified VLAN tag value.

You can use this statement on Gigabit Ethernet IQ, IQ2 and IQ2-E interfaces, 10-Gigabit Ethernet LAN/WAN PIC, for aggregated Ethernet interfaces using Gigabit Ethernet IQ2 and IQ2-E or 10-Gigabit Ethernet PICs on MX Series routers, and for 100-Gigabit Ethernet Type 5 PIC with CFP.

**Required Privilege**  

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

**Related Documentation**  
- Rewriting the Inner and Outer VLAN Tags
**switch-options**

Syntax

```plaintext
switch-options {
  switch-port port-number {
    (auto-negotiation | no-auto-negotiation);
    speed (10m | 100m | 1g);
    link-mode (full-duplex | half-duplex);
  }
}
```

Hierarchy Level

[edit interfaces ge-pim/0/0]

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Configuration of the physical port characteristics is done under the single physical interface.

Required Privilege Level

interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.
switch-port

Syntax

switch-port port-number {
    (auto-negotiation | no-auto-negotiation);
    speed (10m | 100m | 1g);
    link-mode (full-duplex | half-duplex);
}

Hierarchy Level
[edit interfaces ge-pim/0/0 switch-options]

Release Information
Statement introduced in Junos OS Release 8.4.

Description
Configuration of the physical port characteristics, done under the single physical interface.

Default
Autonegotiation is enabled by default. If the link speed and duplex are also configured, the interfaces use the values configured as the desired values in the negotiation.

Options

port-number—Ports are numbered 0 through 5 on the 6-port Gigabit Ethernet uPIM, 0 through 7 on the 8-port Gigabit Ethernet uPIM, and 0 through 15 on the 16-port Gigabit Ethernet uPIM.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege

interface—to view this statement in the configuration.

Level
interface-control—to add this statement to the configuration.
**switch-type**

**Syntax**

```
switch-type (att5e | etsi | nil | ntdms-100)
```

**Hierarchy Level**

```
[edit interfaces br-pim/0/port isdn-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For J Series Services Routers only. Configure the ISDN variant supported.

**Options**

- `att5e`—AT&T switch variant.
- `etsi`—European Telecommunications Standards Institute switch variant.
- `nil`—National ISDN 1 switch variant.
- `ntdms-100`—Northern Telecom DMS-100.
- `ntt`—NTT Group switch for Japan.

**Required Privilege Level**

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

**Related Documentation**

- *Junos OS Interfaces and Routing Configuration Guide*
switching-mode

Syntax

switching-mode (bidirectional | unidirectional);

Hierarchy Level

[edit interfaces interface-name sonet-options aps]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For unchannelized OC3, OC12, and OC48 SONET/SDH interfaces on T Series routers only, configure the interface to interoperate with SONET/SDH line-terminating equipment (LTE) that is provisioned for unidirectional linear APS in 1+1 architecture.

Default

If the `switching-mode` statement is not configured, the mode is bidirectional, and the interface does not interoperate with a unidirectional SONET/SDH LTE.

Options

bidirectional—Support bidirectional mode only.

unidirectional—Interoperate with a SONET/SDH LTE provisioned for unidirectional mode.

Required Privilege Level

interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

Related Documentation

• Configuring Switching Mode
symbol-period

Syntax  symbol-period count;

Hierarchy Level  [edit protocols oam ethernet link-fault-management action-profile event, link-event-rate],
                 [edit protocols oam link-fault-management interface interface-name event-thresholds]

Release Information  Statement introduced in Junos OS Release 8.4.

Description  Configure the threshold for sending symbol period events or taking the action specified in the action profile.

A symbol error is any symbol code error on the underlying physical layer. The symbol period threshold is reached when the number of symbol errors reaches the configured value within the period window. The default period window is the number of symbols that can be transmitted on the underlying physical layer in 1 second. The window is not configurable.

Options  count—Threshold count for symbol period events.
          Range: 0 through 100

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

Related Documentation  • Configuring Threshold Values for Local Fault Events on an Interface
                       • Configuring Threshold Values for Fault Events in an Action Profile
syslog (Interfaces)

Syntax

```bash
syslog {
    host hostname {
        facility-override facility-name;
        log-prefix prefix-number;
        services priority-level;
    }
}
```

Hierarchy Level  [edit interfaces interface-name services-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For adaptive services interfaces, configure generation of system log messages for the service set. System log information is passed to the kernel for logging in the /var/log directory. Any values configured in the service set definition override these values.

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 • Junos OS Services Interfaces Library for Routing Devices
## syslog (Monitoring)

**Syntax**  
(syslog | no-syslog);

**Hierarchy Level**  
[edit interfaces mo-fpc/pic/port multiservice-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
System logging is enabled by default. The system log information of the Monitoring Services PIC is passed to the kernel for logging in the /var/log directory.

- **syslog**—Enable PIC system logging.
- **no-syslog**—Disable PIC system logging.

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

**Related Documentation**  
- Configuring Multiservice Physical Interface Properties on page 154
- Junos OS Services Interfaces Library for Routing Devices
**syslog (OAM Action)**

**Syntax**
```
syslog;
```

**Hierarchy Level**
```
[edit protocols oam ethernet link-fault-management action-profile action]
```

**Release Information**
Statement introduced in Junos OS Release 8.5 for T, M, MX and ACX Series routers, SRX Series firewalls and EX Series switches.
Statement introduced in Junos OS Release 9.4 for EX Series switches and NFX Series devices.

**Description**
Generate a syslog message for the Ethernet Operation, Administration, and Management (OAM) event.

Generate a system log message for the Ethernet Operation, Administration, and Maintenance (OAM) link fault management (LFM) event.

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

**Related Documentation**
- Specifying the Actions to Be Taken for Link-Fault Management Events
- Configuring Ethernet OAM Link Fault Management
system-priority

Syntax

system-priority priority;

Hierarchy Level

[edit interfaces aeX aggregated-ether-options lacp]

Release Information

Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.4 for EX Series switches.
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

Description

Define LACP system priority at the aggregated Ethernet interface level. This system priority value takes precedence over a system priority value configured at the global [edit chassis] hierarchy level.

The device with the lower system priority value determines which links between LACP partner devices are active and which are in standby for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored. In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 127), the device MAC address determines which switch is in control.

Options

priority—Priority for the aggregated Ethernet system. A smaller value indicates a higher priority.

Range: 0 through 65535

Default: 127

Required Privilege

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
t1-options

Syntax  

```
t1-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  buildout value;
  byte-encoding (nx56 | nx64);
  crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
  crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
  fcs (16 | 32);
  framing (esf | sf);
  idle-cycle-flag (flags | ones);
  invert-data;
  line-encoding (ami | b8zs);
  loopback (local | payload | remote);
  remote-loopback-respond;
  start-end-flag (filler | shared);
  timeslots time-slot-range;
}
```

Hierarchy Level  

[edit interfaces interface-name]

Release Information  

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description  

Configure T1-specific physical interface properties.
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  

• T1 Interfaces Overview
t310

**Syntax**  
t310-value seconds;

**Hierarchy Level**  
[edit interfaces br-pim/0/port isdn-options]

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For ISDN interfaces, configure the Q.931-specific timer for T310, in seconds. The Q.931 protocol is involved in the setup and termination of connections.

**Options**  
*seconds*—Timer value, in seconds.

- **Range:** 1 through 65,536 seconds
- **Default:** 10 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 Interfaces and Routing Configuration Guide
t391

Syntax  t391 seconds;

Hierarchy Level  [edit interfaces interface-name mifr-uni-nni-bundle-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For link services and voices interfaces only, set Frame Relay link integrity polling interval.

Options  seconds—Link integrity polling interval.
Range:  5 through 30 seconds
Default:  10 seconds

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

Related Documentation  •  n391 on page 809
•  n392 on page 810
•  n393 on page 811
•  t392 on page 1040
•  Junos OS Services Interfaces Library for Routing Devices
Syntax  
\texttt{t392 seconds;}

Hierarchy Level  
[edit interfaces \texttt{interface-name m1fr-uni-nni-bundle-options}]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For link services and voices interfaces only, set Frame Relay polling verification interval.

Options  
\textit{seconds}—Polling verification interval.  
\textbf{Range}: 5 through 30 seconds  
\textbf{Default}: 15 seconds

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

Related Documentation  
- n391 on page 809  
- n392 on page 810  
- n393 on page 811  
- t391 on page 1039  
- timeslots on page 1050  
- \textit{Junos OS Services Interfaces Library for Routing Devices}
t3-options

Syntax

```
t3-options {
  atm-encapsulation (direct | pici);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
  fcs (16 | 32);
  (feac-loop-respond | no-feac-loop-respond);
  idle-cycle-flag value;
  (long-buildout | no-long-buildout);
  (loop-timing | no-loop-timing);
  loopback (local | payload | remote);
  start-end-flag value;
}
```

Hierarchy Level  [edit interfaces interface-name]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure T3-specific physical interface properties, including the properties of DS3 channels on a channelized OC12 interface. The long-buildout statement is not supported for DS3 channels on a channelized OC12 interface.

On T3 interfaces, the default encapsulation is PPP.

For ATM1 interfaces, you can configure a subset of E3 options statements.

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

- T3 Interfaces Overview
**tag-protocol-id (TPIDs Expected to Be Sent or Received)**

**Syntax**
tag-protocol-id [tpids];

**Hierarchy Level**
[edit interfaces interface-name gigether-options ethernet-switch-profile],
[edit interfaces interface-name aggregated-ether-options ethernet-switch-profile],
[edit interfaces interface-name aggregated-ether-options ethernet-switch-profile],
[edit interfaces interface-name ether-options ethernet-switch-profile]

**Release Information**
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.  
Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.

**Description**
For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces, aggregated Ethernet with Gigabit Ethernet IQ interfaces, and Gigabit Ethernet PICs with SFPs (except the 10-port Gigabit Ethernet PIC, and the built-in Gigabit Ethernet port on the M7i router), define the TPIDs expected to be sent or received on a particular VLAN. For each Gigabit Ethernet port, you can configure up to eight TPIDs using the `tag-protocol-id` statement; but only the first four TPIDs are supported on IQ2 and IQ2-E interfaces.

For 10-Gigabit Ethernet LAN/WAN PIC interfaces on T Series routers only the default TPID value (0x8100) is supported.

For Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces on EX Series switches, define the TPIDs expected to be sent or received on a particular VLAN. The default TPID value is 0x8100. Other supported values are 0x88a8, 0x9100, and 0x9200.

**Options**
**tpids**—TPIDs to be accepted on the VLAN. Specify TPIDs in hexadecimal.

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

**Related Documentation**
- Configuring Frames with Particular TPIDs to Be Processed as Tagged Frames
- Configuring Q-in-Q Tunneling on EX Series Switches with ELS Support
tag-protocol-id (TPID to Rewrite)

Syntax

```
tag-protocol-id tpid;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number input-vlan-map],
[edit interfaces interface-name unit logical-unit-number output-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number input-vlan-map],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number output-vlan-map]
```

Release Information


Description

For Gigabit Ethernet IQ and 10-Gigabit Ethernet IQ2 and IQ2-E interfaces only, configure the outer TPID value. All TPIDs you include in input and output VLAN maps must be among those you specify at the `edit interfaces interface-name gigether-options ethernet-switch-profile tag-protocol-id [tpids]` hierarchy level.

For 10-Gigabit Ethernet LAN/WAN PIC interfaces on T Series routers the default TPID value (0x8100) is supported.

Default

If the `tag-protocol-id` statement is not configured, the TPID value is 0x8100.

Required Privilege

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

Related Documentation

- Configuring Inner and Outer TPIDs and VLAN IDs
**targeted-broadcast**

Syntax (EX Series, MX Series, ACX Series)

```plaintext
targeted-broadcast {
  forward-and-send-to-re;
  forward-only;
}
```

Syntax (QFX Series, OCX1100, EX4600, NFX Series)

```plaintext
targeted-broadcast;
```

Hierarchy Level (EX Series, MX Series, ACX Series)

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]
```

Hierarchy Level (QFX Series, OCX1100, EX4600, NFX Series)

```plaintext
[edit interfaces interface-name unit logical-unit-number family inet],
[edit interfaces interface-range interface-range-name unit logical-unit-number family inet]
```

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 10.2.
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

Specify the IP packets destined for a Layer 3 broadcast address to be forwarded to both an egress interface and the Routing Engine, or to an egress interface only. The packets are broadcast only if the egress interface is a LAN interface.

The remaining statements are explained separately. See CLI Explorer.

Default

When this statement is not included, broadcast packets are sent to the Routing Engine only.

Required Privilege Level

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

Related Documentation

- Configuring Targeted Broadcast on page 251
- Understanding Targeted Broadcast on page 250
targeted-distribution (Static Interfaces over Aggregated Ethernet)

Syntax  targeted-distribution;

Hierarchy Level  [edit interfaces demux0 unit logical-unit-number],
                  [edit interfaces pp0 unit logical-unit-number]

Release Information  Statement introduced in Junos OS Release 11.2.
                        Statement introduced in Junos OS Release 13.2R2 for EX Series switches.

Description  Configure egress data for a logical interface to be sent across a single member link in an
              aggregated Ethernet bundle. A backup link is provisioned and CoS scheduling resources
              are switched to the backup link in the event that the primary assigned link goes down.
              The aggregated Ethernet interface must be configured without link protection.

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

Related Documentation  • CoS for PPPoE Subscriber Interfaces Overview
                        • Configuring the Distribution Type for PPPoE Subscribers on Aggregated Ethernet Interfaces
                        • Verifying the Distribution of PPPoE Subscribers in an Aggregated Ethernet Interface
                        • Targeted Traffic Distribution on Aggregated Ethernet Interfaces in a Virtual Chassis
                        • Configuring Module Redundancy for a Virtual Chassis
                        • Configuring Chassis Redundancy for a Virtual Chassis
## tei-option

**Syntax**

tei-option (first-call | power-up);

**Hierarchy Level**

[edit interfaces br-pim/0/portisdn-options ]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ISDN interfaces, configure when the Terminal Endpoint Identifier (TEI) negotiates with the ISDN provider.

**Options**

- **first-call**—Activation does not occur until the call setup is sent.
- **power-up**—Activation occurs when the Services Router is powered on.

**Default:** power-up

**Required Privilege**

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

**Related Documentation**

- Junos OS Interfaces and Routing Configuration Guide
### terminate (PPPoE Service Name Tables)

**Syntax**

```
terminate;
```

**Hierarchy Level**

```
[edit protocols pppoe service-name-tables table-name service service-name],
[edit protocols pppoe service-name-tables table-name service service-name agent-specifier aci circuit-id-string ari remote-id-string]
```

**Release Information**


**Description**

Direct the router to immediately respond to a PPPoE Active Discovery Initiation (PADI) control packet received from a PPPoE client by sending the client a PPPoE Active Discovery Offer (PADO) packet. The PADO packet contains the name of the access concentrator (router) that can service the client request. The `terminate` action is the default action for a named service entry, `empty` service entry, `any` service entry, or agent circuit identifier/agent remote identifier (ACI/ARI) pair in a PPPoE service name table.

**Required Privilege Level**

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

**Related Documentation**

- `Configuring PPPoE Service Name Tables`
then

<table>
<thead>
<tr>
<th>Syntax</th>
<th>then { discard; }</th>
</tr>
</thead>
</table>

| Hierarchy Level | [edit firewall hierarchical-policer aggregate], [edit firewall hierarchical-policer premium] |

| Release Information | Statement introduced in Junos OS Release 9.5. |

| Description | On M40e, M120, and M320 (with FFPC and SFPC) edge routers and T320, T640, and T1600 core routers with Enhanced Intelligent Queuing (IQE) PICs, discard packets when a specified bandwidth or burst limits for an aggregate level of a hierarchical policer is reached. |

| Options | discard—Discard packets if condition is met. |

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

| Related Documentation | Applying Policers on page 210  
Class of Service Feature Guide (Routers and EX9200 Switches) |
threshold

Syntax    threshold bytes;

Hierarchy Level    [edit interfaces interface-name]

Release Information    Statement introduced before Junos OS Release 7.4.

Description    Specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time, the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate.

Options    bytes—Maximum size, in bytes, for traffic bursts. For ease of entry, you can enter number either as a complete decimal number or as a decimal number followed by the abbreviation k (1000). For example, the entry threshold 2k corresponds to a threshold of 2000 bytes.

Range: 0 through 65,535 bytes

Required Privilege    interface—to view this statement in the configuration.

Level    interface-control—to add this statement to the configuration.

Related Documentation    • Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140
timeslots

Syntax  
timeslots time-slot-range;

Hierarchy Level  
[edit interfaces e1-fpc/pic/port],
[edit interfaces t1-fpc/pic/port],
[edit interfaces interface-name e1-options],
[edit interfaces interface-name partition partition-number],
[edit interfaces interface-name t1-options]

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For E1 and T1 interfaces, allocate the specific time slots by number.

NOTE: When configuring E1 or T1 interfaces on the 10-port Channelized E1/T1 IQ EPIC, the timeslots statement must be included at the [edit interfaces e1-fpc/pic/port] or [edit interfaces t1-fpc/pic/port] hierarchy level as appropriate.

Options  
time-slot-range—Actual time slot numbers allocated:

Range: Ranges vary by interface type and configuration option as follows:

- 1 through 24 for T1 interfaces (0 is reserved)
- 1 through 31 for 4-port E1 PICs (0 is reserved)
- 1 through 31 for Nx DS0 interfaces (0 is reserved)
- 2 through 32 for 10-port Channelized E1 and 10-port Channelized E1 IQ PICs (1 is reserved)
- 2 through 32 for the setting under e1-options with IQE PICs (1 is reserved) (when creating fractional E1)
- 1 through 31 for the setting under partition with IQE PICs (0 is reserved) (when creating Nx DS0)

NOTE: When creating fractional E1 interfaces only, if you connect a 4-port E1 PIC interface to a device that uses time slot numbering from 2 through 32, you must subtract 1 from the configured number of time slots.

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

- Configuring Fractional E1 IQ and IQE Interfaces
- Configuring Fractional T1 IQ and IQE Interfaces
- Configuring Fractional E1 Time Slots
- Configuring Fractional T1 Time Slots
- Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots

**tm**

**Syntax**

```
tm (ignore | normal | require);
```

**Hierarchy Level**

```
[edit interfaces interface-name serial-options dce-options],
[edit interfaces interface-name serial-options dte-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For EIA-530 interfaces only, configure the from-DCE signal, test-mode (TM).

**Options**

- **ignore**—The from-DCE signal is ignored.
- **normal**—Normal TM signal handling as defined by the TIA/EIA Standard 530.
- **require**—The from-DCE signal must be asserted.

**Default:** normal

**Required Privilege Level**

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

**Related Documentation**

- Configuring the Serial Signal Handling on page 324
**tm-polarity**

**Syntax**

```
    tm-polarity (negative | positive);
```

**Hierarchy Level**

```
[edit interfaces interface-name serial-options]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure TM signal polarity.

**Options**

- **negative**—Negative signal polarity.
- **positive**—Positive signal polarity.

**Default:** positive

**Required Privilege Level**

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

**Related Documentation**

- Configuring Serial Signal Polarities on page 327
traceoptions (Individual Interfaces)

**List of Syntax**

- Syntax (Individual interfaces with PTX Series, EX Series, ACX Series) on page 1053
- Syntax (Individual interfaces with QFX Series, OCX1100, EX4600, NFX Series) on page 1053
- Syntax (OAMLFM with EX Series, QFX Series, NFX Series) on page 1053
- Syntax (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series) on page 1053

**Syntax (Individual interfaces with PTX Series, EX Series, ACX Series)**

```
traceoptions {  
  file "filename <files <size <world-readable | no-world-readable>;  
  flag flag;  
  match;  
}
```

**Syntax (Individual interfaces with QFX Series, OCX1100, EX4600, NFX Series)**

```
traceoptions {  
  flag flag;  
}
```

**Syntax (OAMLFM with EX Series, QFX Series, NFX Series)**

```
traceoptions {  
  file "filename <files number <match regex <size <world-readable |  
  no-world-readable>;  
  flag flag;  
  no-remote-trace;  
}
```

**Syntax (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series)**

```
traceoptions {  
  file "filename <files number <match regular-expression <size <world-readable |  
  no-world-readable>;  
  flag flag <disable>;  
  no-remote-trace;  
}
```

**Hierarchy Level**

(Individual interfaces with PTX Series, EX Series, ACX Series, QFX Series, OCX1100, EX4600, NFX Series)

- [edit interfaces interface-name]

(Interface process with ACX Series, SRX Series, MX Series, M Series, T Series)

- [edit interfaces]
### 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 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in JUNOS Release 10.2 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
Define tracing operations for individual interfaces.

To specify more than one tracing operation, include multiple `flag` statements.

The interfaces `traceoptions` statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system `syslog` file in the directory `/var/log/dcd`.

On EX Series, QFX Series, and NFX Series platforms, configure tracing options the link fault management.

On ACX Series, SRX Series, MX Series, M Series, and T Series platforms define tracing operations for the interface process (dcd).

### Default
If you do not include this statement, no interface-specific tracing operations are performed.
Options  Table 28 on page 1056 lists options for traceoption command for the following platforms:
Table 28: Options for traceoptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual Interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with OAM LF with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, TSeries</th>
</tr>
</thead>
<tbody>
<tr>
<td>file filename</td>
<td>—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 <code>/var/log/dcd</code> . By default, interface process tracing output is placed in the file.</td>
<td>—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 <code>/var/log/dcd</code> .</td>
<td>—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 <code>/var/log/dcd</code> . By default, interface process tracing output is placed in the file <code>dcd</code>.</td>
<td></td>
</tr>
<tr>
<td>files number</td>
<td>—(Optional) Maximum number of trace files. When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</td>
<td>—(Optional) Maximum number of trace files. When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>size</code> option.</td>
<td>—(Optional) Maximum number of trace files. When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>size</code> option.</td>
<td></td>
</tr>
<tr>
<td>flag</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. The following are the interface-specific tracing options.</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. The following are the interface-specific tracing options.</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. You can include the following flags:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• all—All interface tracing operations</td>
<td>• action-profile—Trace action profile invocation events.</td>
<td>• all—All interface tracing operations</td>
<td>• all—All interface tracing operations</td>
</tr>
<tr>
<td></td>
<td>• event—Interface events</td>
<td>• change-events—Log changes that produce configuration events</td>
<td>• event—Interface events</td>
<td>• change-events—Log changes that produce configuration events</td>
</tr>
<tr>
<td></td>
<td>• ipc—Interface interprocess</td>
<td>• configuration—Trace configuration events.</td>
<td>• ipc—Interface interprocess</td>
<td>• configuration—Trace configuration events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• protocol—Trace</td>
<td></td>
<td>• protocol—Trace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) Maximum number of trace files. When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>size</code> option.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Range: 2 through 1000

Default: 3 files
### Table 28: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with QAMLFM with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>communication (IPC) messages</td>
<td>protocol processing events.</td>
<td>state machine changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>media</strong>—Interface media changes</td>
<td>• <strong>routing socket</strong>—Trace routing socket events.</td>
<td>• <strong>kernel</strong>—Log configuration IPC messages to kernel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>q921</strong>—Trace ISDN Q.921 frames</td>
<td></td>
<td>• <strong>kernel-detail</strong>—Log details of configuration messages to kernel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>q931</strong>—Trace ISDN Q.931 frames</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>match</strong></td>
<td>(Optional) Regular expression for lines to be traced.</td>
<td>(Optional) Refine the output to log only those lines that match the given regular expression.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>size size</strong></td>
<td>(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <code>trace-file</code> reaches this size, it is renamed <code>trace-file.0</code>. When the <code>trace-file</code> again reaches its maximum size, <code>trace-file.0</code> is renamed <code>trace-file.1</code> and <code>trace-file</code> is renamed <code>trace-file.0</code>. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</td>
<td>(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>file</code> option.</td>
<td>(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>file</code> option.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:** `xk` to specify KB, `xm` 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.
Table 28: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with OAMLFM with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-world-readable</td>
<td>— (Optional) Prevent any user from reading the log file.</td>
<td>— (Optional) Restrict file access to the user who created the file.</td>
<td>— (Optional) Disallow any user to read the log file.</td>
<td>— (Optional) Prevent any user from reading the log file.</td>
</tr>
<tr>
<td>world-readable</td>
<td>— (Optional) Allow any user to read the log file.</td>
<td>— (Optional) Enable unrestricted file access.</td>
<td>— (Optional) Allow any user to read the log file.</td>
<td>— (Optional) Allow any user to read the log file.</td>
</tr>
<tr>
<td>disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

— (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.

Syntax: `xk` to specify kilobytes, `xm` to specify megabytes, or `xg` to specify gigabytes

Range: 10 KB through the maximum file size supported on your router

Default: 1 MB
Table 28: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Interface process with PTX Series, ACX Series, EX Series</th>
<th>Individual Interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with OAMLFM with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-remote-trace</td>
<td>—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</td>
<td>—(Optional) Disable the remote trace.</td>
<td>—(Optional) Disable the remote trace.</td>
<td>—(Optional) Disable the remote trace.</td>
</tr>
<tr>
<td>match regex</td>
<td>—(Optional) Refine the output to include only those lines that match the given regular expression.</td>
<td>—(Optional) Refine the output to include only those lines that match the given regular expression.</td>
<td>—(Optional) Refine the output to include only those lines that match the given regular expression.</td>
<td>—(Optional) Refine the output to include only those lines that match the given regular expression.</td>
</tr>
</tbody>
</table>

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

**Related Documentation**
- Tracing Operations of an Individual Router Interface on page 335
- Tracing Operations of an Individual Router or Switch Interface
- Example: Configuring Ethernet OAM Link Fault Management
- Configuring Ethernet OAM Link Fault Management
- Tracing Operations of the Interface Process on page 336
traceoptions (Individual Interfaces)

List of Syntax

Syntax (Individual interfaces with PTX Series, EX Series, ACX Series) on page 1060
Syntax (Individual interfaces with QFX Series, OCX1100, EX4600, NFX Series) on page 1060
Syntax (OAMLFM with EX Series, QFX Series, NFX Series) on page 1060
Syntax (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series) on page 1060

Syntax (Individual interfaces with PTX Series, EX Series, ACX Series)

traceoptions {
  file filename <files name> <size size> <world-readable | no-world-readable>;
  flag flag;
  match;
}

Syntax (Individual interfaces with QFX Series, OCX1100, EX4600, NFX Series)

traceoptions {
  flag flag;
}

Syntax (OAMLFM with EX Series, QFX Series, NFX Series)

traceoptions {
  file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
  flag flag ;
  no-remote-trace;
}

Syntax (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series)

traceoptions {
  file <filename> <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
  flag flag <disable>;
  no-remote-trace;
}

Hierarchy Level (Individual interfaces with PTX Series, EX Series, ACX Series, QFX Series, OCX1100, EX4600, NFX Series)

[edit interfaces interface-name]

Hierarchy Level (Interface process with ACX Series, SRX Series, MX Series, M Series, T Series)

[edit interfaces]
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 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in JUNOS Release 10.2 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
Define tracing operations for individual interfaces.

To specify more than one tracing operation, include multiple flag statements.

The interfaces traceoptions statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system syslog file in the directory /var/log/dcd.

On EX Series, QFX Series, and NFX Series platforms, configure tracing options the link fault management.

On ACX Series, SRX Series, MX Series, M Series, and T Series platforms define tracing operations for the interface process (dcd).

Default
If you do not include this statement, no interface-specific tracing operations are performed.
Options   Table 28 on page 1056 lists options for traceoption command for the following platforms:
Table 29: Options for traceoptions

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual Interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with OAMLFM with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>file filename</td>
<td>—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 <code>/var/log/dcd</code>. By default, interface process tracing output is placed in the file.</td>
<td>—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 <code>/var/log/dcd</code>.</td>
<td>—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 <code>/var/log/dcd</code>. By default, interface process tracing output is placed in the file <code>dcd</code>.</td>
<td></td>
</tr>
<tr>
<td>files number</td>
<td>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</td>
<td>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>size</code> option.</td>
<td>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, 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 <code>size</code> option.</td>
<td></td>
</tr>
<tr>
<td>flag</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. The following are the interface-specific tracing options.</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. The following are the interface-specific tracing options.</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. You can include the following flags:</td>
<td>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. You can include the following flags:</td>
</tr>
<tr>
<td></td>
<td>• all—All interface tracing operations</td>
<td>• all—All interface tracing operations</td>
<td>• action-profile—Trace action profile invocation events.</td>
<td>• all</td>
</tr>
<tr>
<td></td>
<td>• event—Interface events</td>
<td>• event—Interface events</td>
<td>• change-events—Log changes that produce configuration events</td>
<td>• change-events</td>
</tr>
<tr>
<td></td>
<td>• ipc—Interface interprocess</td>
<td>• ipc—Interface interprocess</td>
<td>• configuration—Trace configuration events.</td>
<td>• configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• protocol—Trace</td>
<td>• protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• config-states—Log the configuration</td>
</tr>
</tbody>
</table>

- Range: 2 through 1000
- Default: 3 files
### Table 29: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with QAMLMF with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match</strong></td>
<td>communication (IPC) messages</td>
<td>communication (IPC) messages</td>
<td>protocol processing events.</td>
<td>state machine changes</td>
</tr>
<tr>
<td></td>
<td>• media—Interface media changes</td>
<td>• media—Interface media changes</td>
<td>• routing socket—Trace routing socket events.</td>
<td>• kernel—Log configuration IPC messages to kernel</td>
</tr>
<tr>
<td></td>
<td>• q921—Trace ISDN Q.921 frames</td>
<td>• q921—Trace ISDN Q.921 frames</td>
<td></td>
<td>• kernel-detail—Log details of configuration messages to kernel</td>
</tr>
<tr>
<td></td>
<td>• q931—Trace ISDN Q.931 frames</td>
<td>• q931—Trace ISDN Q.931 frames</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>size size</strong></td>
<td>—(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.</td>
<td>—(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.</td>
<td>—(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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>—(Optional) Refine the output to log only those lines that match the given regular expression.</td>
<td>—(Optional) Refine the output to log only those lines that match the given regular expression.</td>
<td>—(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.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:** xk to specify KB, xm 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.
### Table 29: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Individual interfaces with PTX Series, ACX Series, EX Series</th>
<th>Individual interfaces with QFX Series, QFabric System, OCX1100, EX4600, NFX Series</th>
<th>Interface Process with QAMLFM with EX Series, QFX Series, NFX Series</th>
<th>Interface process with ACX Series, SRX Series, MX Series, M Series, T Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-world-readable</td>
<td>— (Optional) Prevent any user from reading the log file.</td>
<td>— (Optional) Restrict file access to the user who created the file.</td>
<td>— (Optional) Disallow any user to read the log file.</td>
<td></td>
</tr>
<tr>
<td>world-readable</td>
<td>— (Optional) Allow any user to read the log file.</td>
<td>— (Optional) Enable unrestricted file access.</td>
<td>— (Optional) Allow any user to read the log file.</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

— (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.

**Syntax:** `xk` to specify kilobytes, `xm` to specify megabytes, or `xg` to specify gigabytes

**Range:** 10 KB through the maximum file size supported on your router

**Default:** 1 MB
Table 29: Options for traceoptions (continued)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no-remote-trace</td>
<td>(Optional) Disable the remote trace.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>match regex</td>
<td>(Optional) Refine the output to include only those lines that match the given regular expression.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Related Documentation**
- Tracing Operations of an Individual Router Interface on page 335
- Tracing Operations of an Individual Router or Switch Interface
- Example: Configuring Ethernet OAM Link Fault Management
- Configuring Ethernet OAM Link Fault Management
- Tracing Operations of the Interface Process on page 336
### traceoptions (LACP)

**Syntax**

```plaintext
traceoptions {
  file <filename> <files number> <size size> <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
```

**Hierarchy Level**

[edit protocols lacp]

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 15.1F4 for PTX Series routers.

**Description**

Define tracing operations for the LACP protocol.

**Default**

If you do not include this statement, no LACP protocol tracing operations are performed.

**Options**

- **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, interface process tracing output is placed in the file `lacpd`.

- **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**—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:

  - **all**—All LACP tracing operations
  - **configuration**—Configuration code
  - **packet**—Packets sent and received
  - **process**—LACP process events
  - **protocol**—LACP protocol state machine
  - **routing-socket**—Routing socket events
  - **startup**—Process startup events

  **no-world-readable**—(Optional) Prevent any user from reading the log 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 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:

**Syntax:** `xk` to specify kilobytes, `xm` to specify megabytes, or `xg` to specify gigabytes

**Range:** 10 KB through the maximum file size supported on your router

**Default:** 1 MB

**world-readable**—(Optional) Allow any user to read the log file.

---

**Required Privilege**

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

**Related Documentation**

- *Tracing LACP Operations*
traceoptions (PPP Process)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    level severity-level;
    no-remote-trace;
}
```

Hierarchy Level<br>[edit protocols ppp]

Release Information<br>Statement introduced in Junos OS Release 7.5.

Description<br>Define tracing operations for the PPP process.

To specify more than one tracing operation, include multiple flag statements.

You cannot specify a separate trace tile. Tracing information is placed in the system syslog file in the directory /var/log/pppd.

Default<br>If you do not include this statement, no PPPD-specific tracing operations are performed.

Options

- **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, commit script process tracing output is placed in the file ppd. If you include the file statement, you must specify a filename. To retain the default, you can specify eventd as the 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

- **disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

- **flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the PPPD-specific tracing options.

   - **access**—Access code
• **address-pool**—Address pool code
• **alt**—All areas of code
• **auth**—Authentication code
• **chap**—Challenge Handshake Authentication Protocol (CHAP) code
• **config**—Configuration code
• **ifdb**—Interface database code
• **lcp**—LCP state machine code
• **memory**—Memory management code
• **message**—Message processing code
• **mlppp**—Trace MLPPP code
• **ncp**—NCP state machine code
• **pap**—Password Authentication Protocol (PAP) code
• **ppp**—PPP protocol processing code
• **radius**—RADIUS processing code
• **rtsock**—Routing socket code
• **session**—Session management code
• **signal**—Signal handling code
• **timer**—Timer code
• **ui**—User interface code

**match regex**—(Optional) Refine the output to include only those lines that match the given regular expression.

**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:** `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.

**non-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. Specify `non-world-readable` to reset the default.
Required Privilege Level

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

Related Documentation

- Tracing Operations of the pppd Process on page 137
traceoptions (PPPoE)

Syntax

```
traceoptions {
    file <filename> <files number> <match regular-expression> <size maximum-file-size>
    <world-readable | no-world-readable>;
    filter {
        aci regular-expression;
        ari regular-expression;
        service-name regular-expression;
        underlying-interface interface-name;
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

[edit protocols pppoe]

Release Information

Option filter introduced in Junos OS Release 12.3

Description

Define tracing operations for PPPoE processes.

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

- **disable**—Disable this trace flag.

- **filter**—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

  - **aci regular-expression**—Regular expression to match the agent circuit identifier provided by PPPoE client.

  - **ari regular-expression**—Regular expression to match the agent remote identifier provided by PPPoE client.

  - **service-name regular-expression**—Regular expression to match the service name provided by PPPoE client.

  - **underlying-interface interface-name**—Interface name that the PPPoE client is using.

 **BEST PRACTICE:** Due to the complexity of agent circuit identifiers and agent remote identifiers, we recommend that you do not try an exact match when filtering on these options. For service names, searching on the exact name is appropriate, but you can also use a regular expression with that option.
• **ari regular-expression**—Regular expression to match the agent remote identifier provided by PPPoE client.

• **service regular-expression**—Regular expression to match the name of PPPoE service.

• **underlying-interface interface-name**—Name of a PPPoE underlying interface. You cannot use a regular expression for this filter option.

**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 operations.
- **config**—Trace configuration events.
- **events**—Trace events.
- **gres**—Trace GRES events.
- **init**—Trace initialization events.
- **interface-db**—Trace interface database operations.
- **memory**—Trace memory processing events.
- **protocol**—Trace protocol events.
- **rtsock**—Trace routing socket events.
- **session-db**—Trace connection events and flow.
- **signal**—Trace signal operations.
- **state**—Trace state handling events.
- **timer**—Trace timer processing.
- **ui**—Trace user interface processing.

**level**—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **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.
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 (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: size <size> to specify KB, size <size> to specify MB, or size <size> to specify GB

Range: 10240 through 1073741824

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
- Configuring PPPoE Service Name Tables
- Tracing PPPoE Operations

translate-discard-eligible

Syntax (translate-discard-eligible | no-translate-discard-eligible);

Hierarchy Level
- [edit interfaces <interface-name> unit <logical-unit-number> family ccc],
- [edit logical-systems <logical-system-name> interfaces <interface-name> unit <logical-unit-number> family ccc]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay discard eligible (DE) control bits.

Default
DE bit translation is disabled.

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

Related Documentation
- Configuring Frame Relay Control Bit Translation
translate-fecn-and-becn

Syntax  (translate-fecn-and-becn | no-translate-fecn-and-becn);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For interfaces with encapsulation type Frame Relay CCC, enable or disable translation of Frame Relay forward explicit congestion notification (FECN) control bits and Frame Relay backward explicit congestion notification (BECN) control bits.

Default FECN and BECN bit translation is disabled.

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

Related Documentation • Configuring Frame Relay Control Bit Translation

translate-plp-control-word-de

Syntax translate-plp-control-word-de

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


Description For the interfaces with encapsulation type Frame Relay CCC, classify and rewrite the control word discard eligibility (DE) bit based on the packet loss priority (PLP).

Default PLP bit translation is disabled.

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

Related Documentation • Configuring Frame Relay Control Bit Translation
• frame-relay-de
transmit-bucket

Syntax
transmit-bucket {
  overflow discard;
  rate percentage;
  threshold bytes;
}

Hierarchy Level
[edit interfaces interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Set parameters for the transmit leaky bucket, which specifies what percentage of the interface’s total capacity can be used to transmit packets.

For each DS3 channel in a channelized OC12 interface, you can configure a unique transmit bucket.

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 Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion on page 140
• receive-bucket on page 948
transmit-clock

Syntax  transmit-clock invert;

Hierarchy Level  [edit interfaces interface-name serial-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  Configure the transmit clock signal.

Options  invert—Shift the clock phase 180 degrees.

Required Privilege  level

Level  interface—to view this statement in the configuration.
        interface-control—to add this statement to the configuration.

Related Documentation  • Configuring the Serial Clocking Mode on page 322
transmit-period

Syntax:  transmit-period seconds;

Hierarchy Level:  [edit protocols dot1x authenticator interface interface-id]

Release Information:  Statement introduced in Junos OS Release 9.3.

Description:  Set the number of seconds the port waits before retransmitting the initial EAPOL PDUs to the client.

Options:

  seconds—The number of seconds the port waits before retransmitting the initial EAPOL PDUs to the client.

  Range: 1 through 65,535 seconds

  Default: 30 seconds

Required Privilege Level:

  interface—To view this statement in the configuration.

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

Related Documentation:

  •  IEEE 802.1x Port-Based Network Access Control Overview

  •  authenticator on page 434

  •  dot1x on page 534

  •  interface (IEEE 802.1x) on page 687
transmit-weight (ATM2 IQ CoS Forwarding Class)

Syntax	transmit-weight (cells number | percent number);

Hierarchy Level	[edit interfaces interface-name atm-options scheduler-maps map-name forwarding-class
class-name]

Release Information	Statement introduced before Junos OS Release 7.4.

Description	For ATM2 IQ interfaces only, assign a transmission weight to a forwarding class.

Default	95 percent for queue 0, 5 percent for queue 3.

Options
tp  per  cent  percent—Transmission weight of the forwarding class as a percentage of the
total bandwidth.
Range: 5 through 100

cells number—Transmission weight of the forwarding class as a number of cells.
Range: 0 through 32,000

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

Related Documentation
• ATM2 IQ VC Tunnel CoS Components Overview
transmit-weight (ATM2 IQ Virtual Circuit)

Syntax  
transmit-weight number;

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

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For ATM2 IQ PICs only, configure the transmission weight.

Each VC is serviced in weighted round robin (WRR) mode. When VCs have data to send, they send the number of cells equal to their weight before passing control to the next active VC. This allows proportional bandwidth sharing between multiple VCs within a rate-shaped VP tunnel. VP tunnels are not supported on multipoint interfaces.

Options  
number—Number of cells a VC sends before passing control to the next active VC within a VP tunnel.

Range: 1 through 32,767

Required Privilege Level  
interface—To view this statement in the configuration.

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

Related Documentation  
• Configuring the ATM2 IQ Transmission Weight
## traps

**Syntax**

```
(traps | no-traps);
```

**Hierarchy Level (ACX Series, MX Series, T Series, M Series, SRX Series, EX Series)**

- `[edit dynamic-profiles profile-name interfaces interface-name]`
- `[edit interfaces interface-name]`
- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit interfaces interface-range name]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

**Hierarchy Level (QFX Series, EX4600)**

- `[edit interfaces interface-name]`
- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit interfaces interface-range interface-range-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 12.2 for ACX Series Universal Metro Routers.  
Support at the `[edit dynamic-profiles profile-name interfaces interface-name]` hierarchy level introduced in Junos OS Release 15.1R3 on MX Series routers for enhanced subscriber management.

**Description**

Enable or disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.  

(Enhanced subscriber management for MX Series routers) To enable SNMP notifications, you must first configure the `interface-mib` statement at the `[edit dynamic-profiles profile-name interfaces interface-name]` hierarchy level. If `interface-mib` is not configured, the `traps` statement has no effect.

**BEST PRACTICE:** To achieve maximum performance when enhanced subscriber management is enabled, we recommend that you not enable SNMP notifications on all dynamic subscriber interfaces.

**Required Privilege Level**

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

**Related Documentation**

- [Enabling or Disabling SNMP Notifications on Physical Interfaces on page 155](#)
- [Enabling or Disabling SNMP Notifications on Logical Interfaces on page 185](#)
trigger

**Syntax**

```
trigger {
    defect ignore;
    defect hold-time up milliseconds down milliseconds;
}
```

**Hierarchy Level**

```
[edit interfaces interface-name sonet-options]
```  

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM over SONET/SDH, SONET/SDH interfaces, and 10-Gigabit Ethernet interfaces in WAN PHY mode, configure SONET/SDH defect triggers to be ignored.

**Default**

If you do not include this statement, all SONET/SDH defect triggers are honored.

**Options**

**defect**—Defect to ignore or hold. It can be one of the following:

- ais-l—Line alarm indication signal
- ais-p—Path alarm indication signal
- ber-sd—Bit error rate signal degrade
- ber-sf—Bit error rate signal fault
- locd (ATM only)—Loss of cell delineation
- lof—Loss of frame
- lol—PHY loss of light
- lop-p—Path loss of pointer
- los—Loss of signal
- pll—PHY phase-locked loop out of lock
- plm-p—Path payload (signal) label mismatch
- rfi-l—Line remote failure indication
- rfi-p—Path remote failure indication
- uneq-p—Path unequipped

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.
trigger-link-failure

Syntax

```
[trigger-link-failure interface-name];
```

Hierarchy Level

```
[edit interfaces lsq-fpc/pic/port lsq-failure-options]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

List of SONET interfaces connected to the LSQ interface that can implement Automatic Protection Switching (APS) if the LSQ PIC fails.

Options

- `interface-name`—Name of SONET interface.

Required Privilege Level

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

Related Documentation

- Junos OS Services Interfaces Library for Routing Devices
- Configuring SONET/SDH Defect Triggers
trunk-bandwidth

Syntax  
trunk-bandwidth rate;

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

Release Information  
Statement introduced before Junos OS Release 7.4.

Description  
For ATM2 IQ interfaces configured to use Layer 2 circuit trunk mode, configure a scheduler so that unused bandwidth from any inactive trunk is proportionally shared among the active trunks.

During congestion, each trunk receives a proportional share of the leftover bandwidth, thus minimizing the latency on each trunk.

Options  
rate—Peak rate, in bits per second (bps) or cells per second (cps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

Range: 1,000,000 through 542,526,792 bps

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

Related Documentation  
- Configuring Layer 2 Circuit Trunk Mode Scheduling Overview
trunk-id

**Syntax**

```
trunk-id number;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For ATM2 IQ interfaces with ATM CCC cell-relay encapsulation, configure the trunk identification number.

When you associate a trunk ID number with a logical interface, you are in effect specifying the interfaces that are allowed to send ATM traffic over an LSP.

**Options**

- `number`—A valid trunk identifier.
  
  **Range:** For UNI mode, 0 through 7. For NNI mode, 0 through 31.

**Required Privilege Level**

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

**Related Documentation**

- [Configuring Layer 2 Circuit Transport Mode](#)
ttl

Syntax  ttl value;

Hierarchy Level  [edit interfaces interface-name unit number tunnel]

Release Information  Statement introduced before Junos OS Release 7.4

Description  Set the time-to-live value bit in the header of the outer IP packet.

Options  value—Time-to-live value.
  Range: 0 through 255
  Default: 64

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

Related Documentation
  • Junos OS Services Interfaces Library for Routing Devices
tunnel

Syntax

tunnel {
  backup-destination address;
  destination address;
  key number;
  routing-instance {
    destination routing-instance-name;
  }
  source source-address;
  ttl number;
}

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or VPNs.

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
• Junos OS Services Interfaces Library for Routing Devices
• Junos OS VPNs Library for Routing Devices
underlying-interface

Syntax

underlying-interface interface-name;

Hierarchy Level

[edit interfaces pp0 unit logical-unit-number pppoe-options],
[edit interfaces demux0 unit logical-unit-number demux-options],
[edit logical-systems logical-system-name interfaces demux0 unit logical-unit-number demux-options],
[edit logical-systems logical-system-name interfaces pp0 unit logical-unit-number pppoe-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name interfaces demux0 unit logical-unit-number demux-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name interfaces pp0 unit logical-unit-number pppoe-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Support for aggregated Ethernet added in Junos OS Release 9.4.

Description

Configure the interface on which PPP over Ethernet is running.

For demux interfaces, configure the underlying interface on which the demultiplexing (demux) interface is running.

Options

interface-name—Name of the interface on which PPP over Ethernet or demux is running.

For example, at-0/0/1.0 (ATM VC), fe-1/0/1.0 (Fast Ethernet interface), ge-2/0/0.0 (Gigabit Ethernet interface), ae1.0 (for IP demux on an aggregated Ethernet interface), or ae1 (for VLAN demux on an aggregated Ethernet interface).

NOTE: Demux interfaces are currently supported on Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet interfaces, or aggregated Ethernet devices.

Required Privilege Level

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

Related Documentation

• Configuring an IP Demultiplexing Interface on page 296
• Configuring a VLAN Demultiplexing Interface on page 301
• Configuring the PPPoE Underlying Interface
• Junos OS Interfaces and Routing Configuration Guide
### unframed

**Syntax**

`(unframed | no-unframed);`

**Hierarchy Level**

`[edit interfaces interface-name e3-options]`

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For E3 IQ interfaces only, enable or disable unframed mode. In unframed mode, the E3 IQ interface do not detect yellow (`ylw`) or loss-of-frame (`lof`) alarms.

**Default**

Unframed mode is disabled.

**Required Privilege Level**

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

**Related Documentation**

- Configuring E3 IQ and IQE Unframed Mode
**unidirectional**

Syntax  
unidirectional;

Hierarchy Level  
[edit interfaces interface-name],  
[edit logical-systems logical-system-name interfaces interface-name]

Release Information  
Statement introduced in Junos OS Release 8.5.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  
Create two new, unidirectional (transmit-only and receive-only) physical interfaces subordinate to the original parent interface. Unidirectional links are currently supported only on 10-Gigabit Ethernet interfaces on the following hardware:

- 4-port 10-Gigabit Ethernet DPC on the MX960 router
- 10–Gigabit Ethernet IQ2 PIC and 10–Gigabit Ethernet IQ2E PIC on the T Series router

Default  
Disabled.

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

Related Documentation  
- Understanding Unidirectional Traffic Flow on Physical Interfaces on page 141
- Enabling Unidirectional Traffic Flow on Physical Interfaces on page 142
unit (Dynamic Profiles Standard Interface)

Syntax

```plaintext
unit logical-unit-number {
  actual-transit-statistics;
  auto-configure {
    agent-circuit-identifier {
      dynamic-profile profile-name;
    }
    line-identity {
      include {
        accept-no-ids;
        circuit-id;
        remote-id;
      }
      dynamic-profile profile-name;
    }
  }
  dial-options {
    ipsec-interface-id name;
    l2tp-interface-id name;
    (shared | dedicated);
  }
  encapsulation { atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-tcc-vc-mux |
    atm-mippp-llc | atm-nlpid | atm-ppp-vc-mux | atm-ppp-vc-mux | atm-snap | atm-tcc-snap |
    atm-vc-mux | ether-over-atom-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr |
    ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc |
    frame-relay-ether-type | frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end |
    multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc |
    vlan-vci-ccc | vlan-tcc | vlan-vpls);
  family family {
    address address;
    demux-destination,
    filter {
      adf {
        counter;
        input-precedence precedence;
        not-mandatory;
        output-precedence precedence;
        rule rule-value;
      }
      input filter-name {
        precedence precedence;
        shared-name filter-shared-name;
      }
      output filter-name {
        precedence precedence;
        shared-name filter-shared-name;
      }
    }
    max-sessions number;
    max-sessions-vsa-ignore;
    rpf-check {
      fail-filter filter-name;
    }
  }
}
```

Copyright © 2019, Juniper Networks, Inc.
mode loose;
}
service {
    input {
        service-set service-set-name {
            service-filter filter-name;
        }
        post-service-filter filter-name;
    }
    input-vlan-map {
        inner-tag-protocol-id tpid;
        inner-vlan-id number;
        (push | swap);
        tag-protocol-id tpid;
        vlan-id number;
    }
    output {
        service-set service-set-name {
            service-filter filter-name;
        }
    }
    output-vlan-map {
        inner-tag-protocol-id tpid;
        inner-vlan-id number;
        (pop | swap);
        tag-protocol-id tpid;
        vlan-id number;
    }
}
service-name-table table-name
    short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max maximum-seconds>;
unnumbered-address interface-name <preferred-source-address address>;
}
filter {
    input filter-name {
        shared-name filter-shared-name;
    }
    output filter-name {
        shared-name filter-shared-name;
    }
}
host-prefix-only;
keepalives {
    interval seconds;
}
ppp-options {
  aaa-options aaa-options-name;
  authentication [ authentication-protocols ];
  chap {
    challenge-length minimum minimum-length maximum maximum-length;
    local-name name;
  }
  ignore-magic-number-mismatch;
  initiate-ncp (dual-stack-passive | ipv6 | ip);
  ipcp-suggest-dns-option;
  mru size;
  mtu (size | use-lower-layer);
  on-demand-ip-address;
  pap;
  peer-ip-address-optional;
  local-authentication {
    password password;
    username-include {
      circuit-id;
      delimiter character;
      domain-name name;
      mac-address;
      remote-id;
    }
  }
}

service {
  pcef pcef-profile-name {
    activate rule-name | activate-all;
  }
}

targeted-options {
  backup backup;
  group group;
  primary primary;
  weight ($junos-interface-target-weight | weight-value);
}

vlan-id number;

Hierarchy Level  [edit dynamic-profiles profile-name interfaces interface-name]


Description  Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options

logical-unit-number—The specific unit number of the interface you want to assign to the dynamic profile, or one of the following predefined variables:

- $junos-underlying-interface-unit—For static VLANs, the unit number variable. The static unit number variable is dynamically replaced with the client unit number when the client session begins. The client unit number is specified by the DHCP when it accesses the subscriber network.

- $junos-interface-unit—The unit number variable on a dynamic underlying VLAN interface for which you want to enable the creation of dynamic VLAN subscriber interfaces based on the ACI.

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

- Configuring Dynamic Underlying VLAN Interfaces to Use Agent Circuit Identifier Information
- Configuring Static Underlying VLAN Interfaces to Use Agent Circuit Identifier Information
- Agent Circuit Identifier-Based Dynamic VLANs Overview
unit

Syntax

unit logical-unit-number {
  accept-source-mac {
    mac-address mac-address {
      policer {
        input cos-policer-name;
        output cos-policer-name;
      }
    }
  }
  accounting-profile name;
  advisory-options {
    downstream-rate rate;
    upstream-rate rate;
  }
  allow-any-vci;
  atm-scheduler-map (map-name | default);
  auto-configure {
    agent-circuit-identifier {
      dynamic-profile profile-name;
    }
    line-identity {
      include {
        accept-no-ids;
        circuit-id;
        remote-id;
      }
      dynamic-profile profile-name;
    }
  }
  backup-options {
    interface interface-name;
  }
  bandwidth rate;
  cell-bundle-size cells;
  clear-dont-fragment-bit;
  compression {
    rtp {
      maximum-contexts number <force>;
      f-max-period number;
      queues [queue-numbers];
      port {
        minimum port-number;
        maximum port-number;
      }
    }
    compression-device interface-name;
  }
  copy-tos-to-outer-ip-header;
  demux {
    inet {
      address-source address;
    }
  }
}

Chapter 13: Configuration Statements
auto-configure {
  address-ranges {
    authentication {
      password password-string;
      username-include {
        auth-server-realm realm-string;
        delimiter delimiter-character;
        domain-name domain-name;
        interface-name;
        source-address;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      network ip-address {
        range name {
          low lower-limit;
          high upper-limit;
        }
      }
    }
  }
}
inet6 {
  address-source address;
  auto-configure {
    address-ranges {
      authentication {
        password password-string;
        username-include {
          auth-server-realm realm-string;
          delimiter delimiter-character;
          domain-name domain-name;
          interface-name;
          source-address;
          user-prefix user-prefix-string;
        }
      }
    }
    dynamic-profile profile-name {
      network ip-address {
        range name {
          low lower-limit;
          high upper-limit;
        }
      }
    }
  }
}
demux-destination family;
demux-source family;
demux-options {
  underlying-interface interface-name;
}
description text;
etree-ac-role (leaf | root);
interface {
  l2tp-interface-id name;
  (dedicated | shared);
}
dialer-options {
  activation-delay seconds;
  callback;
  callback-wait-period time;
  deactivation-delay seconds;
  dial-string [dial-string-numbers];
  idle-timeout seconds;
  incoming-map {
    caller caller-id | accept-all;
    initial-route-check seconds;
    load-interval seconds;
    load-threshold percent;
    pool pool-name;
    redial-delay time;
    watch-list {
      [routes];
    }
  }
}
disable;
disable-mlppp-inner-ppp-pfc;
dcli dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold cells plp1 cells;
family family-name {
  ... the family subhierarchy appears after the main [edit interfaces interface-name unit logical-unit-number] hierarchy ...}
fragment-threshold bytes;
host-prefix-only;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
interleave-fragments;
inverse-arp;
layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
}

link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
    up-count cells;
    down-count cells;
}
oam-period (disable | seconds);
output-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
}

passive-monitor-mode;
peer-unit unit-number;
pip-to-clip;
point-to-point;
ppp-options {
    mru size;
    mtu (size | use-lower-layer);
    chap {
        access-profile name;
        default-chap-secret name;
        local-name name;
        passive;
    }
    compression {
        acfc;
        pfc;
    }
    dynamic-profile profile-name;
    ipcp-suggest-dns-option;
lcp-restart-timer milliseconds;
loopback-clear-timer seconds;
ncp-restart-timer milliseconds;
}
pap {
    access-profile name;
    default-pap-password password;
    local-name name;
    local-password password;
    passive;
}
}
pppoe-options {
    access-concentrator name;
    auto-reconnect seconds;
    (client | server);
    service-name name;
    underlying-interface interface-name;
}
pppoe-underlying-options {
    access-concentrator name;
    direct-connect;
    dynamic-profile profile-name;
    max-sessions number;
}
proxy-arp;
service-domain (inside | outside);
shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
    queue-length number;
}
short-sequence;
targeted-distribution;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
vc vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
    access-concentrator name;
    address address [ ... the address subhierarchy appears after the main [edit interfaces interface-name unit logical-unit-number family family-name] hierarchy ... ]
    bundle interface-name;
    core-facing;
    demux-destination {
        destination-prefix;
    }
    demux-source {
        source-prefix;
    }
    direct-connect;
    duplicate-protection;
    dynamic-profile profile-name;
    filter {
        group filter-group-number;
        input filter-name;
        input-list [filter-names];
        output filter-name;
        output-list [filter-names];
    }
    interface-mode (access | trunk);
    ipsec-sa sa-name;
    keep-address-and-control;
    mac-validate (loose | strict);
    max-sessions number;
    mtu bytes;
    multicast-only;
    no-redirects;
    policer {
        arp policer-template-name;
        input policer-template-name;
        output policer-template-name;
    }
    primary;
    protocols [inet iso mpls];
    proxy inet-address address;
    receive-options-packets;
    receive-ttl-exceeded;
    remote (inet-address address | mac-address address);
    rpf-check {
        fail-filter filter-name
        mode loose;
    }
    sampling {
        input;
output;
}

service {
  input {
    post-service-filter filter-name;
    service-set service-set-name <service-filter filter-name>;
  }
  output {
    service-set service-set-name <service-filter filter-name>;
  }
}

service-name-table table-name
targeted-options {
  backup backup;
  group group;
  primary primary;
  weight ($junos-interface-target-weight | weight-value);
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address
destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address [  
arp ip-address (mac | multicast-mac) mac-address <publish>;  
broadcast address;  
destination address;  
destination-profile name;  
eui-64;  
master-only;  
multipoint-destination address [  
dlci dlci-identifier;  
epd-threshold cells <plp1 cells>;  
inverse-arp;  
oam-liveness [  
  up-count cells;  
  down-count cells;  
]  
oam-period (disable | seconds);  
shaping [  
  (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate sustained rate);  
  queue-length number;  
]  
vci vpi-identifier.vci-identifier;  
]  
preferred;  
primary;  
(vrrp-group | vrrp-inet6-group) group-number [  
  (accept-data | no-accept-data);  
  advertise-interval seconds;  
  authentication-type authentication;  
  authentication-key key;  
  fast-interval milliseconds;  
  (preempt | no-preempt) [  
    hold-time seconds;  
  ]  
  priority number;  
  track [  
    interface interface-name [  
      bandwidth-threshold bits-per-second priority-cost number;  
    ]  
  priority-hold-time seconds;  
  route ip-address/prefix-length routing-instance instance-name priority-cost cost;  
]  
virtual-address [addresses];  
virtual-link-local-address ipv6-address;  
vrrp-inherit-from [  
  active-interface interface-name;  
  active-group group-number;  
];  
];  
]
Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

**Options**

- **logical-unit-number**—Number of the logical unit.
  - **Range:** 0 through 1,073,741,823 for demux, PPPoE, and pseudowire static interfaces. 0 through 16,385 for all other static interface types.

- **etree-ac-role (leaf | root)**—To configure an interface as either leaf or root.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
unnumbered-address (Demux)

Syntax

unnumbered-address interface-name <preferred-source-address address>;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family inet],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet]

Release Information

Statement introduced in Junos OS Release 8.2.
preferred-source-address option introduced in Junos OS Release 9.0.
IP demultiplexing interfaces supported in Junos OS Release 9.2.

Description

For IP demultiplexing interfaces, enable the local address to be derived from the specified interface. Configuring an unnumbered interface enables IP processing on the interface without assigning an explicit IP address to the interface.

Options

interface-name—Name of the interface from which the local address is derived. The specified interface must have a logical unit number and a configured IP address, and must not be an unnumbered interface.

The preferred-source-address statement is 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 an Unnumbered Interface on page 202
• address on page 407
• Junos System Basics Configuration Guide
unnumbered-address (Dynamic Profiles)

Syntax

unnumbered-address interface-name <preferred-source-address address>;

Hierarchy Level

[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family family],
[edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family family]

Release Information


Description

For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring unnumbered Ethernet interfaces enables IP processing on the interface without assigning an explicit IP address to the interface. To configure unnumbered address dynamically, include the $junos-loopback-interface-address predefined variable.

You can configure unnumbered address support on Ethernet interfaces for IPv4 and IPv6 address families.

Options

interface-name—Name of the interface from which the local address is derived. The specified interface must have a logical unit number, a configured IP address, and must not be an unnumbered interface. This value can be a specific interface name or the $junos-loopback-interface predefined variable.

When defining the unnumbered-address statement using a static interface, keep the following in mind:

- If you choose to include the routing-instance statement at the [edit dynamic-profiles] hierarchy level, that statement must be configured with a dynamic value by using the $junos-routing-instance predefined variable. In addition, whatever static unnumbered interface you specify must belong to that routing instance; otherwise, the profile instantiation fails.
- If you choose to not include the routing-instance statement at the [edit dynamic-profiles] hierarchy level, the unnumbered-address statement uses the default routing instance. The use of the default routing instance requires that the unnumbered interface be configured statically and that it reside in the default routing instance.

NOTE: When you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the $junos-routing-instance predefined variable, you must not configure a preferred source address, whether with the $junos-preferred-source-address predefined variable, the
preferred-source-address statement. Configuring the preferred source address in this circumstance causes a commit failure.

When defining the unnumbered-address statement using the $junos-loopback-interface predefined variable, keep the following in mind:

- To use the $junos-loopback-interface predefined variable, the dynamic profile must also contain the routing-instance statement configured with the $junos-routing-instance predefined variable at the [edit dynamic-profiles] hierarchy level.
- The applied loopback interface is based on the dynamically obtained routing instance of the subscriber.

address—(Optional) Secondary IP address of the donor interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network. This value can be a static IP address, the $junos-preferred-source-address predefined variable for the inet family, or the $junos-preferred-source-ipv6-address predefined variable for the inet6 family.

When defining the preferred-source-address value using a static IP address, keep the following in mind:

- The unnumbered interface must be statically configured.
- The IP address specified as the preferred-source-address must be configured in the specified unnumbered interface.

When defining the preferred-source-address value using the $junos-preferred-source-address or the $junos-preferred-source-ipv6-address predefined variables, keep the following in mind:

- You must configure the unnumbered-address statement using the $junos-loopback-interface predefined variable.
- You must configure the routing-instance statement using the $junos-routing-instance predefined variable at the [edit dynamic-profiles] hierarchy level.
- The preferred source address chosen is based on the dynamically applied loopback address which is in turn derived from the dynamically obtained routing instance of the subscriber. The configured loopback address with the closest network match to the user IP address is selected as the preferred source address.

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

Related Documentation
- Dynamic Profiles Overview
unnumbered-address (Ethernet)

Syntax
unnumbered-address interface-name <preferred-source-address address>;

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

Release Information
Statement introduced in Junos OS Release 8.2.
preferred-source-address option introduced in Junos OS Release 9.0.

Description
For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring an unnumbered Ethernet interface enables IP processing on the interface without assigning an explicit IP address to the interface.

Options
interface-name—Name of the interface from which the local address is derived. The specified interface must have a logical unit number and a configured IP address, and must not be an unnumbered interface.

The preferred-source-address statement is explained separately.

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

Related Documentation
- Configuring an Unnumbered Interface on page 202
- address on page 407
- Junos System Basics Configuration Guide
unnumbered-address (PPP)

**Syntax**
unnumbered-address interface-name destination address destination-profile profile-name;

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

**Release Information**
Statement introduced before Junos OS Release 7.4.

**Description**
For interfaces with PPP encapsulation, enable the local address to be derived from the specified interface.

**Options**
- *interface-name*—Interface from which the local address is derived. The interface name must include a logical unit number and must have a configured 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**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring IPCP Options for Interfaces with PPP Encapsulation on page 200
up-count

Syntax  up-count cells;

Hierarchy Level  [edit interfaces interface-name atm-options vpi vpi-identifier oam-liveness],
[edit interfaces interface-name unit logical-unit-number oam-liveness],
[edit interfaces interface-name unit logical-unit-number family family address address multipoint-destination address oam-liveness],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number oam-liveness],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address multipoint-destination address oam-liveness]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For ATM encapsulation only, configure Operation, Administration, and Maintenance (OAM) F5 loopback cell count thresholds. Not supported on ATM-over-SHDSL interfaces.

For ATM2 IQ PICs only, configure OAM F4 loopback cell count thresholds at the [edit interfaces interface-name atm-options vpi vpi-identifier] hierarchy level.

Options  cells—Minimum number of consecutive OAM F4 or F5 loopback cells received before a VC is declared up.

Range: 1 through 255

Default: 5 cells

Required Privilege Level  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring the ATM OAM F5 Loopback Cell Threshold
**user-prefix**

**Syntax**

```
user-prefix user-prefix-string;
```

**Hierarchy Level**

[edit interfaces interface-name auto-configure vlan-ranges authentication username-include],
[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication username-include]

**Release Information**

Statement introduced in Junos OS Release 10.0.

**Description**

Specify the user prefix that is concatenated with the username during the subscriber authentication process.

**Options**

```
user-prefix-string—The user prefix string.
```

**Required Privilege Level**

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

**Related Documentation**

- Configuring VLAN Interface Username Information for AAA Authentication
username-include (Interfaces)

**Syntax**

```plaintext
username-include {
    circuit-id;
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name;
    mac-address;
    option-18;
    option-37;
    option-82 <circuit-id> <remote-id>;
    radius-realm radius-realm-string;
    remote-id;
    user-prefix user-prefix-string;
    vlan-tags;
}
```

**Hierarchy Level**

- [edit interfaces interface-name auto-configure vlan-ranges authentication],
- [edit interfaces interface-name auto-configure stacked-vlan-ranges authentication]

**Release Information**

Statement introduced in Junos OS Release 10.0.
`vlan-tags` option added in Junos OS Release 18.3R1 on MX Series routers.

**Description**

Configure the username that the router 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 accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The username takes the format `user-prefix mac-address circuit-type circuit-id remote-id option–82 interface-name domain-name radius-realm`. By default, each component is separated by a period (.), but you can specify a different delimiter with the `delimiter` statement.

**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.

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 remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.
<table>
<thead>
<tr>
<th>Required Privilege</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Configuring VLAN Interface Username Information for AAA Authentication
- Using DHCP Option 82 Suboptions in Authentication Usernames for Autosense VLANs
- Using DHCP Option 18 and Option 37 in Authentication Usernames for DHCPv6 Autosense VLANs
- Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs
vbr

Syntax  vbr peak rate sustained rate burst length;

Hierarchy Level  [edit interfaces interface-name atm-options vpi vpi-identifier shaping],
[edit interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ],
[edit interfaces interface-name unit logical-unit-number shaping ],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number address address family family multipoint-destination address shaping ],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number shaping ]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For ATM encapsulation only, define the variable bandwidth utilization in the traffic-shaping profile.

When you configure the variable bandwidth utilization, you must specify all three options (burst, peak, and sustained). You can specify the rate in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify the rate in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

Default  If the vbr statement is not specified, bandwidth utilization is unlimited.

Options  burst length—Burst length, in cells. If you set the length to 1, the peak traffic rate is used.
Range: 1 through 4000 cells

peak rate—Peak rate, in bits per second or cells per second.
Range: For ATM1 interfaces, 33 Kbps through 135.6 Mbps (ATM OC3); 33 Kbps through 276 Mbps (ATM OC12). For ATM2 IQ OC3 and OC12 interfaces, 33 Kbps through 542,526,792 bps. For ATM2 IQ OC48 interfaces, 33 Kbps through 2,170,107,168 bps. For ATM2 IQ DS3 and E3 interfaces, from 33 Kbps through the maximum rate, which depends on the ATM encapsulation and framing you configure.

sustained rate—Sustained rate, in bits per second or cells per second.
Range: For ATM1 interfaces, 33 Kbps through 135.6 Mbps (ATM OC3); 33 Kbps through 276 Mbps (ATM OC12). For ATM2 IQ OC3 and OC12 interfaces, 33 Kbps through 542,526,792 bps. For ATM2 IQ OC48 interfaces, 33 Kbps through 2,170,107,168 bps. For ATM2 IQ DS3 and E3 interfaces, from 33 Kbps through the maximum rate, which depends on the ATM encapsulation and framing you configure.
vc-cos-mode

Syntax
vc-cos-mode (alternate | strict);

Hierarchy Level
[edit interfaces interface-name atm-options scheduler-maps map-name]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For ATM2 IQ interfaces only, specify packet-scheduling priority value for ATM2 IQ VC tunnels.

Options
- alternate—VC CoS queue has high priority. The scheduling of the queues alternates between the high-priority queue and the remaining queues, so every other scheduled packet is from the high-priority queue.

- strict—VC CoS queue has strictly high priority. A queue with strict high priority is always scheduled before the remaining queues. The remaining queues are scheduled in round-robin fashion.

Default: alternate
vci

Syntax  vci vpi-identifier.vci-identifier;

Hierarchy Level  [edit interfaces at-fpc/pic/port unit logical-unit-number],
                 [edit interfaces at-fpc/pic/port unit logical-unit-number family family address address multipoint-destination address],
                 [edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number],
                 [edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number family family address address multipoint-destination address]

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 12.2 for the ACX Series Universal Metro routers.

Description  For ATM point-to-point logical interfaces only, configure the virtual circuit identifier (VCI) and virtual path identifier (VPI).

To configure a VPI for a point-to-multipoint interface, specify the VPI in the multipoint-destination statement.

VCIs 0 through 31 are reserved for specific ATM values designated by the ATM Forum.

Options  vci-identifier—ATM virtual circuit identifier. Unless you configure the interface to use promiscuous mode, this value cannot exceed the highest-numbered VC configured for the interface with the maximum-vcs option of the vpi statement.

Range: 0 through 4089 or 0 through 65,535 with promiscuous mode, with VCIs 0 through 31 reserved.

vpi-identifier—ATM virtual path identifier.

Range: 0 through 255

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 a Point-to-Point ATM1 or ATM2 IQ Connection
                       • Applying Scheduler Maps to Logical ATM Interfaces
**vci-range**

**Syntax**
```
vci-range start-vci end-vci;
```

**Hierarchy Level**
[edit interfaces at-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number]

**Release Information**
Statement introduced in Junos OS Release 9.0.

**Description**
Range of VCI values used in ATM-to-Ethernet interworking cross-connects. VCI 0 through 31 are reserved. VCI 0 through 31 should not be used.

**Options**
- `start-vci`—Lowest number VCI in the range.
- `end-vci`—Highest number VCI in the range.

**Range:** 0 through 255

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

**Related Documentation**
- Configuring ATM-to-Ethernet Interworking on page 262

**virtual-switch**

**Syntax**
```
virtual-switch name bridge-domain name vlan-id [vlan-ids ];
```

**Hierarchy Level**
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name default-x]

**Release Information**

**Description**
Specify the routing-instance type as a virtual switch, under which bridge-domain MIPs must be enabled.

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

**Related Documentation**
- Configuring MIP for Bridge Domains of a Virtual Switch
vlan-id (Logical Port in Bridge Domain)

**Syntax**

```
vlan-id number;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family bridge],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family bridge]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 15.1.

**Description**

The VLAN ID configured on the logical port. Received packets with no VLAN tags are forwarded within the bridge domain with the matching VLAN ID.

**Options**

- **number**—The VLAN ID.

  **Range:** 1 through 4095

**Required Privilege Level**

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

**Related Documentation**

- Configuring Access Mode on a Logical Interface
- Tunnel Services Overview
- Tunnel Interface Configuration on MX Series Routers Overview
**vlan-id (Outer VLAN ID)**

**Syntax**

`vlan-id outer-vlan-id;`

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced in Junos OS Release 9.0.

**Description**

The outer VLAN ID to be used in ATM-to-Ethernet interworking cross-connects. Outer VLAN IDs are converted to the ATM VPI. The outer VLAN ID must match the VPI value configured. The allowable VPI range is 0 to 255. Do not configure the outer VLAN ID to be greater than 255.

**Options**

- `outer-vlan-id`—Outer VLAN ID number.

  **Range**: 0 through 4094

**Required Privilege Level**

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

**Related Documentation**

- Configuring ATM-to-Ethernet Interworking on page 262
vlan-id (VLAN ID to Be Bound to a Logical Interface)

**Syntax**    
`vlan-id number;`

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

**Release Information**  
Statement introduced before Junos OS Release 7.4.

**Description**  
For Fast Ethernet, Gigabit Ethernet, and Aggregated Ethernet interfaces only, bind a 802.1Q VLAN tag ID to a logical interface.

**Options**  
`number`—A valid VLAN identifier.

**Range:** For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for management and internal Ethernet interfaces, 1 through 1023. In Junos OS Evolved `vlan-id 0` is not supported.

For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094.

VLAN ID 0 is reserved for tagging the priority of frames used in Junos OS. In Junos OS Evolved `vlan-id 0` is not supported.

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

**Related Documentation**  
- Enabling VLAN Tagging
**native-vlan-id**

**Syntax**

native-vlan-id vlan-id;

**Hierarchy Level (QFX Series and EX4600)**

For platforms without ELS:

[edit interfaces (QFX Series) interface-name unit 0 family ethernet-switching]

For platforms with ELS:

[edit interfaces (QFX Series) interface-name]

**Hierarchy Level (ACX Series, EX Series, SRX Series, M Series, MX Series, and T Series)**

[edit interfaces ge-fpc/pic/port],
[edit interfaces interface-name]

**Hierarchy Level (SRX Series)**

[edit interfaces interface-name]

**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 9.5 for SRX Series.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.

**Description**

Configure the VLAN identifier to associate with untagged packets received on the physical interface of a trunk mode interface for the following:

- QFX Series and EX4600
- M Series routers with Gigabit Ethernet IQ PICs with SFP and Gigabit Ethernet IQ2 PICs with SFP configured for 802.1Q flexible VLAN tagging
- MX Series routers with Gigabit Ethernet DPCs and MICs, Tri-Rate Ethernet DPCs and MICs, and 10-Gigabit Ethernet DPCs and MICs and MPCs configured for 802.1Q flexible VLAN tagging
- T4000 routers with 100-Gigabit Ethernet Type 5 PIC with CFP
- EX Series switches with Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces

The logical interface on which untagged packets are received must be configured with the same VLAN ID as the native VLAN ID configured on the physical interface, otherwise the untagged packets are dropped. To configure the logical interface, include the `vlan-id`
statement (matching the `native-vlan-id` statement on the physical interface) at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

When the `native-vlan-id` statement is included with the `flexible-vlan-tagging` statement, untagged packets are accepted on the same mixed VLAN-tagged port and on the interfaces that are configured for Q-in-Q tunneling.

When the `native-vlan-id` statement is combined with the `interface-mode` statement, untagged packets are accepted and forwarded within the bridge domain or VLAN that is configured with the matching VLAN ID.

To configure the logical interface, include the `vlan-id` statement (matching the `native-vlan-id` statement on the physical interface) at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level.

---

**NOTE:** Starting in Junos OS Release 17.1R1, you can send untagged traffic without a native VLAN ID to the remote end of the network. To do this, remove the native VLAN ID from the untagged traffic configuration by setting the `no-native-vlan-insert` statement. If you do not configure this statement, the native VLAN ID is added to the untagged traffic.

---

**Default**

By default, the untagged packets are dropped. That is, if you do not configure the `native-vlan-id` option, the untagged packets are dropped.

**Options**

- `vlan-id`—Numeric identifier of the VLAN.
  - **Range:** 1 through 4094
- `number`—VLAN ID number.
  - **Range:** (ACX Series routers, SRX Series devices and EX Series switches) 0 through 4094.

**Required Privilege Level**

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

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure)
- Understanding Bridging and VLANs on Switches
- Enabling VLAN Tagging
- Configuring Access Mode on a Logical Interface
- Configuring the Native VLAN Identifier on Switches With ELS Support
- Understanding Interfaces
- Understanding Q-in-Q Tunneling and VLAN Translation
- no-native-vlan-insert
- Sending Untagged Traffic Without VLAN ID to Remote End
- show ethernet-switching interfaces
- show vlans
- flexible-vlan-tagging on page 617
- Junos OS Network Interfaces Configuration Guide
**vlan-id-list (Ethernet VLAN Circuit)**

**Syntax**

```
vlan-id-list [vlan-id vlan-id–vlan-id];
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

Binds a single-tag logical interface to a list of VLAN IDs. Configures a logical interface to receive and forward any tag frame whose VLAN ID tag matches the list of VLAN IDs you specify.

**NOTE:**
When you create a circuit cross-connect (CCC) using VLAN-bundled single-tag logical interfaces on Layer 2 VPN routing instances, the circuit automatically uses ethernet encapsulation. For Layer 2 VPN, you need to include the encapsulation-type statement and specify the value ethernet at either of the following hierarchy levels:

- [edit routing-instances routing-instance-name protocols l2vpn]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn]

For more information about the encapsulation-type configuration statement and the Layer 2 encapsulation types ethernet and ethernet-vlan, see the Junos OS VPNs Library for Routing Devices.

**Options**

```
[vlan-id vlan-id–vlan-id]—A list of valid VLAN ID numbers. Specify the VLAN IDs individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both.

Range: 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.
```

**NOTE:** Configuring vlan-id-list with the entire vlan-id range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1-4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:
[edit interfaces interface-name]
    vlan-tagging;
    unit number {
        vlan-id-range 1-4094;
    }

[edit interfaces interface-name]
    unit 0;

---

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

**Related Documentation**
- *Binding VLAN IDs to Logical Interfaces*
- encapsulation (Logical Interface) on page 567
- encapsulation on page 571
- encapsulation-type (Layer 2 VPN routing instance), see the *Junos OS VPNs Library for Routing Devices*
- flexible-vlan-tagging on page 617
- vlan-tagging on page 1131
- vlan-tags (Dual-Tagged Logical Interface) on page 1133
**vlan-id-list (Interface in Bridge Domain)**

**Syntax**

```
vlan-id-list [ number number-number ];
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family bridge],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family bridge]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 15.1.

**Description**

Configure a logical interface to forward packets and learn MAC addresses within each bridge domain configured with a VLAN ID that matches a VLAN ID specified in the list. VLAN IDs can be entered individually using a space to separate each ID, entered as an inclusive list separating the starting VLAN ID and ending VLAN ID with a hyphen, or a combination of both.

**Options**

- `number number`—Individual VLAN IDs separated by a space.
- `number-number`—Starting VLAN ID and ending VLAN ID in an inclusive range.
  
  **Range:** 1 through 4095

**Required Privilege Level**

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

**Related Documentation**

- Configuring a Logical Interface for Trunk Mode
- Configuring the VLAN ID List for a Trunk Interface
- Tunnel Services Overview
- Tunnel Interface Configuration on MX Series Routers Overview
**vlan-id-range**

**Syntax**  
`vlan-id-range vlan-id–vlan-id`

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

**Release Information**  
Statement introduced in Junos OS Release 8.4.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**  
Bind a range of VLAN IDs to a logical interface.

**Options**  
`number`—The first number is the lowest VLAN ID in the range the second number is the highest VLAN ID in the range.

**Range:** 1 through 4094

---

**NOTE:** Configuring `vlan-id-range` with the entire vlan-id range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1-4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]
  vlan-tagging;
  unit number {
    vlan-id-range 1-4094;
  }

[edit interfaces interface-name]
  unit 0;
```

VLAN ID 0 is reserved for tagging the priority of frames.

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

**Related Documentation**  
- Binding a Range of VLAN IDs to a Logical Interface
vlan-ranges

Syntax
vlan-ranges [  
  access-profile profile-name;  
  authentication {  
    packet-types [packet-types];  
    password password-string;  
    username-include {  
      circuit-type;  
      circuit-id;  
      delimiter delimiter-character;  
      domain-name domain-name-string;  
      interface-name;  
      mac-address;  
      option-18;  
      option-37;  
      option-82 <circuit-id> <remote-id>;  
      radius-realm radius-realm-string;  
      remote-id;  
      user-prefix user-prefix-string;  
      vlan-tags;  
    }  
  }  
  dynamic-profile profile-name {  
    accept (any | dhcp-v4 | inet);  
    accept-out-of-band protocol;  
    access-profile vlan-dynamic-profile-name;  
    ranges (any | low-tag)–(any | high-tag);  
  }  
  override;  
]  

Hierarchy Level  [edit interfaces interface-name auto-configure]

Release Information  Statement introduced in Junos OS Release 9.5.

Description  Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.

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  • Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs
                      • Configuring Interfaces to Support Both Single and Stacked VLANs
**Syntax**

```
vlan-rewrite translate (200 500 | 201 501)
```

**Hierarchy Level**

```
[edit interfaces interface-name unit number family bridge interface-mode trunk]
[edit interfaces interface-name unit number family ethernet-switching interface-mode trunk]
```

**Release Information**

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Translates an incoming VLAN to a bridge-domain VLAN, corresponding counter translation at egress. Supports translation of VLAN 200 to VLAN 500 and VLAN 201 to VLAN 501. Other valid VLANs pass through without translation.

**Options**

- `translate 200 500`—Translates incoming packets with VLAN 200 to 500.
- `translate 201 501`—Translates incoming packets with VLAN 201 to 501.

**Required Privilege Level**

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

**Related Documentation**

- *Rewriting a VLAN Tag and Adding a New Tag*
**vlan-rule (100-Gigabit Ethernet Type 4 PIC with CFP)**

**Syntax**

`vlan-rule (high-low | odd-even);`

**Hierarchy Level**

```
[edit chassis fpc slot pic slot forwarding-mode vlan-steering]
```

**Release Information**

Statement introduced in Junos OS Release 10.4.

**Description**

Configure the interoperability mode of the 100-Gigabit Ethernet Type 4 PIC with CFP (PD-1CE-CFP-FPC4) when interoperating with 100 gigabit Ethernet interfaces from other vendors.

If no VLAN rule is configured, all tagged packets are distributed to PFE0.

**Options**

- **high-low**—VLAN IDs 1 through 2047 are distributed to PFE0 and VLAN IDs 2048 through 4096 are distributed to PFE1.
- **odd-even**—Odd number VLAN IDs are distributed to PFE1 and even number VLAN IDs are distributed to PFE0.

**Required Privilege Level**

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

**Related Documentation**

- Configuring VLAN Steering Mode for 100-Gigabit Ethernet Type 4 PIC with CFP
- forwarding-mode (100-Gigabit Ethernet)
- vlan-steering (100-Gigabit Ethernet Type 4 PIC with CFP) on page 1130
**vlan-steering (100-Gigabit Ethernet Type 4 PIC with CFP)**

**Syntax**

```
vlan-steering {
  vlan-rule (high-low | odd-even);
}
```

**Hierarchy Level**

```
[edit chassis fpc slot pic slot forwarding-mode]
```

**Release Information**

Statement introduced in Junos OS Release 9.4.

**Description**

Configure the 100-Gigabit Ethernet Type 4 PIC with CFP (PD-ICE-CFP-FPC4) to interoperate with 100 gigabit Ethernet interfaces from other vendors.

The other statement is 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 VLAN Steering Mode for 100-Gigabit Ethernet Type 4 PIC with CFP
- forwarding-mode (100-Gigabit Ethernet)
- sa-multicast (100-Gigabit Ethernet) on page 975
- vlan-rule (100-Gigabit Ethernet Type 4 PIC with CFP) on page 1129
vlan-tagging

**Syntax**

```
vlan-tagging;
```

**Syntax (QFX Series, NFX Series, and EX4600)**

```
vlan-tagging;
```

**Syntax (SRX Series Interfaces)**

```
vlan-tagging native-vlan-id vlan-id;
```

**Hierarchy Level**

```
[edit interfaces interface-name],
[edit logical-systems logical-system-name interfaces interface-name]
```

**QFX Series, NFX Series, and EX4600 Interfaces**

```
[edit interfaces (QFX Series) interface-name ]
[edit interfaces (QFX Series) interface-range interface-range-name ]
```

**SRX Series Interfaces**

```
[edit interfaces interface ]
```

**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 9.5.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.
Statement introduced in Junos OS Release 13.2 for PTX Series Routers.
Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series.

**Description**

For Fast Ethernet and Gigabit Ethernet interfaces, aggregated Ethernet interfaces configured for VPLS, and pseudowire subscriber interfaces, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.

**NOTE:** For QFX Series configure VLAN identifier for untagged packets received on the physical interface of a trunk mode interface. Enable VLAN tagging. The platform receives and forwards single-tag frames with 802.1Q VLAN tags.

On EX Series switches except for EX4300 and EX9200 switches, the `vlan-tagging` and `family ethernet-switching` statements cannot be configured on the same interface. Interfaces on EX2200, EX3200, EX3300, EX4200, and EX4500 switches are set to `family ethernet-switching` by the default factory configuration. EX6200 and EX8200 switch interfaces do not have a default family setting.
VLAN tagging is disabled by default.

Options

**native-vlan-id**—(SRX Series) Configures a VLAN identifier for untagged packets. Enter a number from 0 through 4094.

---

**NOTE:** The native-vlan-id can be configured only when either flexible-vlan-tagging mode or interface-mode trunk is configured.

---

**Required Privilege Level**

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

**Related Documentation**

- [802.1Q VLANs Overview](#)
- [Configuring a Layer 3 Subinterface (CLI Procedure)](#)
- [Configuring Tagged Aggregated Ethernet Interfaces](#)
- [Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch](#)
- [vlan-id](#)
- [Configuring a Layer 3 Logical Interface](#)
- [Configuring VLAN Tagging](#)
### vlan-tags (Dual-Tagged Logical Interface)

**Syntax**

```plaintext
vlan-tags inner-list [vlan-id vlan-id–vlan-id] outer <tpid.>vlan-id;
```

**Hierarchy Level**

```plaintext
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

(MX Series routers only) Binds a dual-tag logical interface to a list of VLAN IDs. Configures the logical interface to receive and forward any dual-tag frame whose inner VLAN ID tag matches the list of VLAN IDs you specify.

---

**NOTE:**

To create a circuit cross-connect (CCC) using VLAN-bundled dual-tag logical interfaces on Layer 2 VPN routing instances, you must include the encapsulation-type statement and specify the value ethernet-vlan at the one of the following hierarchy levels:

- [edit routing-instances routing-instance-name protocols l2vpn]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn]

For more information about the encapsulation-type configuration statement and the Layer 2 encapsulation types ethernet and ethernet-vlan, see the Junos OS VPNs Library for Routing Devices.

---

**Options**

- **inner-list [vlan-id vlan-id vlan-id–vlan-id]**—A list of valid VLAN ID numbers. Specify the VLAN IDs individually by using a space to separate each ID, as an inclusive list by separating the starting VLAN ID and ending VLAN ID with a hyphen, or as a combination of both.
  - **Range:** 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

- **outer <tpid.>vlan-id**—An optional Tag Protocol ID (TPID) and a valid VLAN ID.
  - **Range:** For TPID, specify a hexadecimal value in the format Oxnnnn.
  - **Range:** For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

**NOTE:** Configuring inner-list with the entire vlan-id range is an unnecessary waste of system resources and is not best practice. It should be used only when a subset of VLAN IDs of inner tag (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1 through 4094), the inner VLAN ID is unnecessary.
4094), it has the same result as not specifying a range; however, it consumes PFE resources such as VLAN lookup tables entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]
vlan-tagging;
unit number {
    vlan-tags outer vid inner-list 1-4094;
}
```

```
[edit interfaces interface-name]
vlan-tagging;
unit number {
    vlan-id vid;
}
```

**Required Privilege**

**Level**

interface—to view this statement in the configuration.

interface-control—to add this statement to the configuration.

**Related Documentation**

- Binding VLAN IDs to Logical Interfaces
- encapsulation (Logical Interface) on page 567
- encapsulation on page 571
- encapsulation-type (Layer 2 VPN routing instance), see the Junos OS VPNs Library for Routing Devices.
- flexible-vlan-tagging on page 617
- vlan-id-list (Ethernet VLAN Circuit) on page 1123
- vlan-tagging on page 1131
vlan-tags (Stacked VLAN Tags)

Syntax

```
_vlan-tags inner tpid vlan-id inner-list value inner-range vid1—vid2 outer tpid vlan-id;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

Description

Bind TPIDs and 802.1Q VLAN tag IDs to a logical interface. TPID fields are used to identify the frame as an IEEE 802.1Q-tagged frame.

Options

- **inner tpid vlan-id**—A TPID and a valid VLAN identifier. TPID is a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.
  - **Range:** For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames. For PTX Series, VLAN ID 0 is not supported.

- **inner-list value**—List or a set of VLAN identifiers.

  **NOTE:** This is supported on MX Series routers with Trio-based FPCs.

- **inner-range tpid vid1—vid2**—Specify a TPID and a range of VLAN IDs where vid1 is the start of the range and vid2 is the end of the range.

  **NOTE:** On the network-to-network (NNI) or egress interfaces of provider edge (PE) routers, you cannot configure the inner-range tpid vid1—vid2 option with the vlan-tags statement for ISP-facing interfaces.

- **Range:** For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

- **outer tpid vlan-id**—A TPID and a valid VLAN identifier.

  **Range:** For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames. For PTX Series, VLAN ID 0 is not supported.

  **NOTE:** Configuring inner-range with the entire vlan-id range consumes system resources and is not a best practice. The inner-range must be used only when a subset of VLAN IDs of inner tag (not the entire range) needs to be associated...
with a logical interface. If you specify the entire range (1 through 4094), it has the same result as not specifying a range; however, it consumes Packet Forwarding Engine resources such as VLAN lookup table entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]
stacked-vlan-tagging;
unit number {
    vlan-tags outer vid inner-range 1-4094;
}

[edit interfaces interface-name]
vlan-tagging;
unit number {
    vlan-id vid;
}
```

**Required Privilege**

- **Level**: interface—To view this statement in the configuration.
- **interface-control—To add this statement to the configuration.**

**Related Documentation**

- Configuring Dual VLAN Tags
- Configuring Flexible VLAN Tagging on PTX Series Packet Transport Routers
- stacked-vlan-tagging on page 1019

**vlan-tags-outer**

**Syntax**

```
vlan-tags-outer vlan-tag;
```

**Hierarchy Level**

```
[edit interfaces interface-set interface-set-name interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.

**Description**

The S-VLAN outer tag that belongs to a set of interfaces used to configure hierarchical CoS schedulers.

**Required Privilege**

- **Level**: interface—To view this statement in the configuration.
- **interface-control—To add this statement to the configuration.**

**Related Documentation**

- Class of Service Feature Guide (Routers and EX9200 Switches)
**vlan-vci-tagging**

**Syntax**
```
vlan-vci-tagging;
```

**Hierarchy Level**
```
[edit interfaces interface-name],
[edit logical-systems logical-system-name interfaces interface-name]
```

**Release Information**
Statement introduced in Junos OS Release 9.0.

**Description**
Enable the ATM-to-Ethernet interworking cross-connect function on a Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interface.

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

**Related Documentation**
- Configuring ATM-to-Ethernet Interworking on page 262

---

**vpi (ATM CCC Cell-Relay Promiscuous Mode)**

**Syntax**
```
vpi vpi-identifier;
```

**Hierarchy Level**
```
[edit interfaces at-fpc/pic/port atm-options promiscuous-mode]
```

**Release Information**

**Description**
For ATM interfaces, allow all VCIs in this VPI to open in ATM CCC cell-relay mode.

When you include `vpi` statements at the [edit interfaces interface-name atm-options promiscuous-mode] hierarchy level, the specified VPIs open in promiscuous mode.

**Options**
- `vpi-identifier`—ATM virtual path identifier. This is one of the VPIs that you define in the `vci` statement. (For a list of hierarchy levels at which you can include the `vci` statement, see `vci`.)

  **Range:** 0 through 255

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

**Related Documentation**
- Configuring ATM Cell-Relay Promiscuous Mode
vpi (Define Virtual Path)

Syntax

```
vpi vpi-identifier {
  maximum-vcs maximum-vcs;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period (disable | seconds);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
    queue-length number;
  }
}
```

Hierarchy Level

[edit interfaces at-fpc/pic/port atm-options]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For ATM interfaces, configure the virtual path (VP).

NOTE: Certain options apply only to specific platforms.

Options

`vpi-identifier`—ATM virtual path identifier. This is one of the VPIs that you define in the `vci` statement. (For a list of hierarchy levels at which you can include the `vci` statement, see `vci`.)

Range: 0 through 255

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

- Configuring the Maximum Number of ATM1 VCs on a VP
## vpi (Logical Interface and Interworking)

**Syntax**  
```
vpi virtual-path-identifier;
```

**Hierarchy Level**  
- [edit interfaces at-fpc/pic/port unit logical-unit-number],
- [edit logical-systems logical-system-name interfaces at-fpc/pic/port unit logical-unit-number]

**Release Information**  
Statement introduced in Junos OS Release 9.0.  
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro routers.

**Description**  
VPI used in an ATM-to-Ethernet interworking cross-connect.

**Options**  
- `virtual-path-identifier`—VPI to be used.  
  - **Range:** 0 through 255

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

**Related Documentation**  
- [Configuring ATM-to-Ethernet Interworking](#) on page 262  
- [Configuring ATM Cell-Relay Promiscuous Mode](#)
vtmapping

Syntax  vtmapping (itu-t | klm);

Hierarchy Level  [edit chassis fpc number pic number],
                [edit interfaces interface-name sonet-options]

Release Information  Statement introduced before Junos OS Release 7.4.

Description  For the Channelized STM1 IQ PIC or Channelized STM1 PIC, configure virtual tributary mapping.

For the Channelized STM1 PIC, you configure virtual tributary mapping at the [edit chassis fpc number pic number] hierarchy level.

NOTE: The vtmapping statement is not supported for cau4 interfaces on the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (H).

Options  itu-t—International Telephony Union standard.

klm—KLM standard.

Default: klm

Required Privilege  interface—To view this statement in the configuration.

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

Related Documentation  • Configuring Virtual Tributary Mapping of Channelized STM1 Interfaces

• Configuring the Junos OS to Support Channelized STM1 Interface Virtual Tributary Mapping
### warning

**Syntax**

```plaintext
warning low-light-warning {
  (link-down | syslog);
}
```

**Hierarchy Level**

[edit interfaces interface-name optics-options]

**Release Information**

- Statement introduced in Junos OS Release 10.0.
- Statement introduced in Junos OS Release 12.1 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for PTX Series routers.
- Statement introduced in Junos OS Release 18.3R1 for PTX10K-LC1104 on the PTX10008 and PTX10016 routers.

**Description**

Specifies the action to take if the receiving optics signal is below the optics low-light warning threshold.

**Options**

- **link-down**—Drop the 10-Gigabit Ethernet link and marks link as down.
- **syslog**—Write the optics information to the system log.

**Required Privilege Level**

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

**Related Documentation**

- [Configuring Link Down Notification for Optics Options Alarm or Warning](#)
- [optics-options on page 855](#)
- [100-Gigabit Ethernet OTN Options Configuration Overview](#)
**watch-list**

**Syntax**
```plaintext
watch-list {
  [ routes ];
}
```

**Hierarchy Level**
```
[edit interfaces dl n unit logical-unit-number dialer-options]
```

**Release Information**
Statement introduced before JunosOS Release 7.4.

**Description**
On J Series Services Routers with ISDN interfaces, configure an ISDN list of routes to watch. Used only for dialer watch.

**Options**
- **routes**—IP prefix of a route. Specify one or more. The primary interface is considered up if there is at least one valid route for any of the addresses in the watch list to an interface other than the backup interface.

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

**Related Documentation**
- Junos OS Interfaces and Routing Configuration Guide
wavelength

Syntax  wavelength nm;

Hierarchy Level  [edit interfaces interface-name optics-options]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series routers.

Description  For 10-Gigabit or 100-Gigabit Ethernet DWDM interfaces only, configure full C-band ITU-Grid tunable optics.

Options  nm—Wavelength value. It can be one of the following:

- 1528.38—1528.38 nanometers (nm), corresponds to a 50-GHz grid
- 1528.77—1528.77 nm, corresponds to 50-GHz and 100-GHz grids
- 1529.16—1529.16 nm, corresponds to a 50-GHz grid
- 1529.55—1529.55 nm, corresponds to 50-GHz and 100-GHz grids
- 1529.94—1529.94 nm, corresponds to a 50-GHz grid
- 1530.33—1530.33 nm, corresponds to 50-GHz and 100-GHz grids
- 1530.72—1530.72 nm, corresponds to a 50-GHz grid
- 1531.12—1531.12 nm, corresponds to 50-GHz and 100-GHz grids
- 1531.51—1531.51 nm, corresponds to a 50-GHz grid
- 1531.90—1531.90 nm, corresponds to 50-GHz and 100-GHz grids
- 1532.29—1532.29 nm, corresponds to a 50-GHz grid
- 1532.68—1532.68 nm, corresponds to 50-GHz and 100-GHz grids
- 1533.07—1533.07 nm, corresponds to a 50-GHz grid
- 1533.47—1533.47 nm, corresponds to 50-GHz and 100-GHz grids
- 1533.86—1533.86 nm, corresponds to a 50-GHz grid
- 1534.25—1534.25 nm, corresponds to 50-GHz and 100-GHz grids

NOTE: All values are displayed. However, if you configure a value that is not supported by the device, an error message is displayed and the device is not tuned to the specified wavelength.
- 1534.64—1534.64 nm, corresponds to a 50-GHz grid
- 1535.04—1535.04 nm, corresponds to 50-GHz and 100-GHz grids
- 1535.43—1535.43 nm, corresponds to a 50-GHz grid
- 1535.82—1535.82 nm, corresponds to 50-GHz and 100-GHz grids
- 1536.22—1536.22 nm, corresponds to a 50-GHz grid
- 1536.61—1536.61 nm, corresponds to 50-GHz and 100-GHz grids
- 1537.00—1537.00 nm, corresponds to a 50-GHz grid
- 1537.40—1537.40 nm, corresponds to 50-GHz and 100-GHz grids
- 1537.79—1537.79 nm, corresponds to a 50-GHz grid
- 1538.19—1538.19 nm, corresponds to 50-GHz and 100-GHz grids
- 1538.58—1538.58 nm, corresponds to a 50-GHz grid
- 1538.98—1538.98 nm, corresponds to 50-GHz and 100-GHz grids
- 1539.37—1539.37 nm, corresponds to a 50-GHz grid
- 1539.77—1539.77 nm, corresponds to 50-GHz and 100-GHz grids
- 1540.16—1540.16 nm, corresponds to a 50-GHz grid
- 1540.56—1540.56 nm, corresponds to 50-GHz and 100-GHz grids
- 1540.95—1540.95 nm, corresponds to a 50-GHz grid
- 1541.35—1541.35 nm, corresponds to 50-GHz and 100-GHz grids
- 1541.75—1541.75 nm, corresponds to a 50-GHz grid
- 1542.14—1542.14 nm, corresponds to 50-GHz and 100-GHz grids
- 1542.54—1542.54 nm, corresponds to a 50-GHz grid
- 1542.94—1542.94 nm, corresponds to 50-GHz and 100-GHz grids
- 1543.33—1543.33 nm, corresponds to a 50-GHz grid
- 1543.73—1543.73 nm, corresponds to 50-GHz and 100-GHz grids
- 1544.13—1544.13 nm, corresponds to a 50-GHz grid
- 1544.53—1544.53 nm, corresponds to 50-GHz and 100-GHz grids
- 1544.92—1544.92 nm, corresponds to a 50-GHz grid
- 1545.32—1545.32 nm, corresponds to 50-GHz and 100-GHz grids
- 1545.72—1545.72 nm, corresponds to a 50-GHz grid
- 1546.12—1546.12 nm, corresponds to 50-GHz and 100-GHz grids
- 1546.52—1546.52 nm, corresponds to a 50-GHz grid
- 1546.92—1546.92 nm, corresponds to 50-GHz and 100-GHz grids
- 1547.32—1547.32 nm, corresponds to a 50-GHz grid
• 1547.72—1547.72 nm, corresponds to 50-GHz and 100-GHz grids
• 1548.11—1548.11 nm, corresponds to a 50-GHz grid
• 1548.51—1548.51 nm, corresponds to 50-GHz and 100-GHz grids
• 1548.91—1548.91 nm, corresponds to a 50-GHz grid
• 1549.32—1549.32 nm, corresponds to 50-GHz and 100-GHz grids
• 1549.72—1549.72 nm, corresponds to a 50-GHz grid
• 1550.12—1550.12 nm, corresponds to 50-GHz and 100-GHz grids
• 1550.52—1550.52 nm, corresponds to a 50-GHz grid
• 1551.12—1551.12 nm, corresponds to 50-GHz and 100-GHz grids
• 1551.52—1551.52 nm, corresponds to a 50-GHz grid
• 1552.93—1552.93 nm, corresponds to a 50-GHz grid
• 1553.33—1553.33 nm, corresponds to 50-GHz and 100-GHz grids
• 1553.73—1553.73 nm, corresponds to a 50-GHz grid
• 1554.13—1554.13 nm, corresponds to 50-GHz and 100-GHz grids
• 1554.54—1554.54 nm, corresponds to a 50-GHz grid
• 1554.94—1554.94 nm, corresponds to 50-GHz and 100-GHz grids
• 1555.34—1555.34 nm, corresponds to a 50-GHz grid
• 1555.75—1555.75 nm, corresponds to 50-GHz and 100-GHz grids
• 1556.15—1556.15 nm, corresponds to a 50-GHz grid
• 1556.55—1556.55 nm, corresponds to 50-GHz and 100-GHz grids
• 1556.95—1556.95 nm, corresponds to a 50-GHz grid
• 1557.36—1557.36 nm, corresponds to 50-GHz and 100-GHz grids
• 1557.77—1557.77 nm, corresponds to a 50-GHz grid
• 1558.17—1558.17 nm, corresponds to 50-GHz and 100-GHz grids
• 1558.58—1558.58 nm, corresponds to a 50-GHz grid
• 1558.98—1558.98 nm, corresponds to 50-GHz and 100-GHz grids
• 1559.39—1559.39 nm, corresponds to a 50-GHz grid
• 1559.79—1559.79 nm, corresponds to 50-GHz and 100-GHz grids
• 1560.20—1560.20 nm, corresponds to a 50-GHz grid
• 1560.61—1560.61 nm, corresponds to 50-GHz and 100-GHz grids
• 1561.01—1561.01 nm, corresponds to a 50-GHz grid
• 1561.42—1561.42 nm, corresponds to 50-GHz and 100-GHz grids
• 1561.83—1561.83 nm, corresponds to a 50-GHz grid
• 1562.23—1562.23 nm, corresponds to 50-GHz and 100-GHz grids
• 1562.64—1562.64 nm, corresponds to a 50-GHz grid
• 1563.05—1563.05 nm, corresponds to 50-GHz and 100-GHz grids
• 1563.45—1563.45 nm, corresponds to a 50-GHz grid
• 1563.86—1563.86 nm, corresponds to 50-GHz and 100-GHz grids
• 1564.27—1564.27 nm, corresponds to a 50-GHz grid
• 1564.68—1564.68 nm, corresponds to 50-GHz and 100-GHz grids
• 1565.09—1565.09 nm, corresponds to a 50-GHz grid
• 1565.50—1565.50 nm, corresponds to 50-GHz and 100-GHz grids
• 1565.90—1565.90 nm, corresponds to a 50-GHz grid
• 1566.31—1566.31 nm, corresponds to 50-GHz and 100-GHz grids
• 1566.72—1566.72 nm, corresponds to a 50-GHz grid
• 1567.13—1567.13 nm, corresponds to 50-GHz and 100-GHz grids
• 1567.54—1567.54 nm, corresponds to a 50-GHz grid
• 1567.95—1567.95 nm, corresponds to 50-GHz and 100-GHz grids
• 1568.36—1568.36 nm, corresponds to a 50-GHz grid
• 1568.77—1568.77 nm, corresponds to 50-GHz and 100-GHz grids

Default: 1550.12—1550.12 nm, corresponds to 50-GHz and 100-GHz grids

Required Privilege Level

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

Related Documentation

• Ethernet DWDM Interface Wavelength Overview
• Configuring the 10-Gigabit or 100-Gigabit Ethernet DWDM Interface Wavelength
• show interfaces diagnostics optics (Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, 100-Gigabit Ethernet, and Virtual Chassis Port)
west-interface

Syntax

```
west-interface [  
ode-id mac-address;  
control-channel channel-name {  
  vlan number;  
  interface name interface-name  
}  
interface-none  
ring-protection-link-end;  
virtual-control-channel {  
  west-interface name;  
  east-interface name;  
}  
}
```

Hierarchy Level
[edit protocols protection-group ethernet-ring ring-name]

Release Information
Statement introduced in Junos OS Release 9.5.  
Statement introduced in Junos OS Release 12.1 for EX Series switches.  

Description
Define one of the two interface ports for Ethernet ring protection, the other being defined by the east-interface statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

NOTE: Always configure this port second, after configuring the east-interface statement.

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
- Ethernet Ring Protection Switching Overview
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- east-interface on page 564
- ethernet-ring on page 591
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS
working-circuit

Syntax

```
working-circuit group-name;
```

Hierarchy Level

```
[edit interfaces interface-name sonet-options aps]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the working router in an APS circuit pair.

Options

```
group-name—Circuit’s group name.
```

Required Privilege Level

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

Related Documentation

- Configuring Basic Automatic Protect Switching
- protect-circuit on page 928
**yellow-differential-delay**

**Syntax**

yellow-differential-delay milliseconds;

**Hierarchy Level**

[edit interfaces interface-name mlfr-uni-nni-bundle-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

For link services and voices interfaces only, configure the yellow differential delay among bundle links to give warning when a link has a differential delay that exceeds the configured threshold.

**Options**

- **milliseconds**—Yellow differential delay threshold.
  - **Range:** 1 through 2000 milliseconds
  - **Default:** 6 milliseconds

**Required Privilege Level**

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

**Related Documentation**

- Junos OS Services Interfaces Library for Routing Devices
- action-red-differential-delay on page 404
- remote on page 953
**z0-increment**

**Syntax**

(z0-increment | no-z0-increment);

**Hierarchy Level**

[edit interfaces interface-name sonet-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.

**Description**

Configure an incremental STM ID rather than a static one.

**Default**

no-z0-increment

**Required Privilege**

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

**Related Documentation**

- Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode
- sonet-options on page 1002
CHAPTER 14

Interface Operational Commands

- Common Output Fields Description on page 1152
- Improvements to Interface Transmit Statistics Reporting on page 1160
- show interfaces
- show interfaces (ATM)
- show interfaces (Channelized DS3-to-DS0)
- show interfaces (Channelized DS3-to-DS1)
- show interfaces (Channelized E1 IQ)
- show interfaces (Channelized E1)
- show interfaces (Channelized OC12 IQ and IQE)
- show interfaces (Channelized OC12)
- show interfaces (Channelized OC3 IQ and IQE)
- show interfaces (Channelized STM1 IQ)
- show interfaces (Channelized STM1)
- show interfaces (Channelized T1 IQ)
- show interfaces (Channelized T3 IQ)
- show interfaces (Discard)
- show interfaces (Fast Ethernet)
- show interfaces
- show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)
- show interfaces (PPPoE)
- show interfaces (PTX Series Packet Transport Routers)
- show interfaces (SONET/SDH)
- show interfaces (Serial)
- show interfaces (T1, E1, or DS)
- show interfaces (T3 or E3)
- show interfaces demux0 (Demux Interfaces)
- show interfaces extensive
• show interfaces lsi (Label-Switched Interface)
• show interfaces media
• show interfaces terse

Common Output Fields Description

This chapter explains the content of the output fields, which appear in the output of most show interfaces commands.

Damping Field

For the physical interface, the Damping field shows the setting of the following damping parameters:

• **half-life**—Decay half-life. The number of seconds after which the accumulated interface penalty counter is reduced by half if the interface remains stable.

• **max-suppress**—Maximum hold-down time. The maximum number of seconds that an interface can be suppressed irrespective of how unstable the interface has been.

• **reuse**—Reuse threshold. When the accumulated interface penalty counter falls below this number, the interface is no longer suppressed.

• **suppress**—Cutoff (suppression) threshold. When the accumulated interface penalty counter exceeds this number, the interface is suppressed.

• **state**—Interface damping state. If damping is enabled on an interface, it is suppressed during interface flaps that match the configured damping parameters.

Destination Class Field

For the logical interface, the Destination class field provides the names of destination class usage (DCU) counters per family and per class for a particular interface. The counters display packets and bytes arriving from designated user-selected prefixes. For example:

<table>
<thead>
<tr>
<th>Destination class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>1928095 (889)</td>
<td>161959980 (597762)</td>
</tr>
<tr>
<td>bronze</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Enabled Field

For the physical interface, the Enabled field provides information about the state of the interface, displaying one or more of the following values:

- **Administratively down, Physical link is Down**—The interface is turned off, and the physical link is inoperable and cannot pass packets even when it is enabled. To change the interface state to Enabled, use the following command:

  ```bash
  user@host# set interfaces interface enable
  ```

  Manually verify the connections to bring the physical link up.

- **Administratively down, Physical link is Up**—The interface is turned off, but the physical link is operational and can pass packets when it is enabled. To change the interface state to Enabled, use the following command:

  ```bash
  user@host# set interfaces interface enable
  ```

- **Enabled, Physical link is Down**—The interface is turned on, but the physical link is inoperable and cannot pass packets. Manually verify the connections to bring the physical link up.

- **Enabled, Physical link is Up**—The interface is turned on, and the physical link is operational and can pass packets.

Filters Field

For the logical interface, the Filters field provides the name of the firewall filters to be evaluated when packets are received or transmitted on the interface. The format is Filters: Input: filter-name and Filters: Output: filter-name. For example:

```plaintext
Filters: Input: sample-all
Filters: Output: cp-ftp
```

Flags Fields

The following sections provide information about flags that are specific to interfaces:

- Addresses, Flags Field on page 1154
- Device Flags Field on page 1154
- Family Flags Field on page 1155
- Interface Flags Field on page 1156
- Link Flags Field on page 1156
- Logical Interface Flags Field on page 1157
Addresses, Flags Field

The **Addresses, Flags** field provides information about the addresses configured for the protocol family on the logical interface and displays one or more of the following values:

- **Dest-route-down**—The routing process detected that the link was not operational and changed the interface routes to nonforwarding status.
- **Is-Default**—The default address of the router used as the source address by SNMP, ping, traceroute, and other network utilities.
- **Is-Preferred**—The default local address for packets originating from the local router and sent to destinations on the subnet.
- **Is-Primary**—The default local address for broadcast and multicast packets originated locally and sent out the interface.
- **Preferred**—This address is a candidate to become the preferred address.
- **Primary**—This address is a candidate to become the primary address.
- **Trunk**—Interface is a trunk.
- **Trunk, Inter-Switch-Link**—Interface is a trunk, and InterSwitch Link protocol (ISL) is configured on the trunk port of the primary VLAN in order to connect the routers composing the PVLAN to each other.

Device Flags Field

The **Device flags** field provides information about the physical device and displays one or more of the following values:

- **ASIC Error**—Device is down because of ASIC wedging and due to which PFE is disabled.
- **Down**—Device has been administratively disabled.
- **Hear-Own-Xmit**—Device receives its own transmissions.
- **Link-Layer-Down**—The link-layer protocol has failed to connect with the remote endpoint.
- **Loopback**—Device is in physical loopback.
- **Loop-Detected**—The link layer has received frames that it sent, thereby detecting a physical loopback.
- **No-Carrier**—On media that support carrier recognition, no carrier is currently detected.
- **No-Multicast**—Device does not support multicast traffic.
- **Present**—Device is physically present and recognized.
- **Promiscuous**—Device is in promiscuous mode and recognizes frames addressed to all physical addresses on the media.
- **Quench**—Transmission on the device is quenched because the output buffer is overflowing.
• **Recv-All-Multicasts**—Device is in multicast promiscuous mode and therefore provides no multicast filtering.

• **Running**—Device is active and enabled.

**Family Flags Field**

The **Family flags** field provides information about the protocol family on the logical interface and displays one or more of the following values:

• **DCU**—Destination class usage is enabled.

• **Dest-route-down**—The software detected that the link is down and has stopped forwarding the link's interface routes.

• **Down**—Protocol is inactive.

• **Is-Primary**—Interface is the primary one for the protocol.

• **Mac-Validate-Loose**—Interface is enabled with loose MAC address validation.

• **Mac-Validate-Strict**—Interface is enabled with strict MAC address validation.

• **Maximum labels**—Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.

• **MTU-Protocol-Adjusted**—The effective MTU is not the configured value in the software.

• **No-Redirects**—Protocol redirects are disabled.

• **Primary**—Interface can be considered for selection as the primary family address.

• **Protocol-Down**—Protocol failed to negotiate correctly.

• **SCU-in**—Interface is configured for source class usage input.

• **SCU-out**—Interface is configured for source class usage output.

• **send-bcast-packet-to-re**—Interface is configured to forward IPv4 broadcast packets to the Routing Engine.

• **targeted-broadcast**—Interface is configured to forward IPv4 broadcast packets to the LAN interface and the Routing Engine.

• **Unnumbered**—Protocol family is configured for unnumbered Ethernet. An unnumbered Ethernet interface borrows an IPv4 address from another interface, which is referred to as the donor interface.

• **Up**—Protocol is configured and operational.

• **uRPF**—Unicast Reverse Path Forwarding is enabled.
Interface Flags Field

The interface flags field provides information about the physical interface and displays one or more of the following values:

- **Admin-Test**—Interface is in test mode and some sanity checking, such as loop detection, is disabled.
- **Disabled**—Interface is administratively disabled.
- **Down**—A hardware failure has occurred.
- **Hardware-Down**—Interface is nonfunctional or incorrectly connected.
- **Link-Layer-Down**—Interface keepalives have indicated that the link is incomplete.
- **No-Multicast**—Interface does not support multicast traffic.
- **No-receive No-transmit**—Passive monitor mode is configured on the interface.
- **OAM-On-SVLAN**—(MX Series routers with MPC/MIC interfaces only) Interface is configured to propagate the Ethernet OAM state of a static, single-tagged service VLAN (S-VLAN) on a Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interface to a dynamic or static double-tagged customer VLAN (C-VLAN) that has the same S-VLAN (outer) tag as the S-VLAN.
- **Point-To-Point**—Interface is point-to-point.
- **Pop all MPLS labels from packets of depth**—MPLS labels are removed as packets arrive on an interface that has the pop-all-labels statement configured. The depth value can be one of the following:
  - 1—Takes effect for incoming packets with one label only.
  - 2—Takes effect for incoming packets with two labels only.
  - [12]—Takes effect for incoming packets with either one or two labels.
- **Promiscuous**—Interface is in promiscuous mode and recognizes frames addressed to all physical addresses.
- **Recv-All-Multicasts**—Interface is in multicast promiscuous mode and provides no multicast filtering.
- **SNMP-Traps**—SNMP trap notifications are enabled.
- **Up**—Interface is enabled and operational.

Link Flags Field

The link flags field provides information about the physical link and displays one or more of the following values:

- **ACFC**—Address control field compression is configured. The Point-to-Point Protocol (PPP) session negotiates the ACFC option.
- **Give-Up**—Link protocol does not continue connection attempts after repeated failures.
• **Loose-LCP**—PPP does not use the Link Control Protocol (LCP) to indicate whether the link protocol is operational.

• **Loose-LMI**—Frame Relay does not use the Local Management Interface (LMI) to indicate whether the link protocol is operational.

• **Loose-NCP**—PPP does not use the Network Control Protocol (NCP) to indicate whether the device is operational.

• **No-Keepalives**—Link protocol keepalives are disabled.

• **PFC**—Protocol field compression is configured. The PPP session negotiates the PFC option.

**Logical Interface Flags Field**

The *Logical interface flags* field provides information about the logical interface and displays one or more of the following values:

• **ACFC Encapsulation**—Address control field Compression (ACFC) encapsulation is enabled (negotiated successfully with a peer).

• **Device-down**—Device has been administratively disabled.

• **Disabled**—Interface is administratively disabled.

• **Down**—A hardware failure has occurred.

• **Clear-DF-Bit**—GRE tunnel or IPsec tunnel is configured to clear the Don’t Fragment (DF) bit.

• **Hardware-Down**—Interface protocol initialization failed to complete successfully.

• **PFC**—Protocol field compression is enabled for the PPP session.

• **Point-To-Point**—Interface is point-to-point.

• **SNMP-Traps**—SNMP trap notifications are enabled.

• **Up**—Interface is enabled and operational.

**Label-Switched Interface Traffic Statistics Field**

When you use the *vrf-table-label* statement to configure a VRF routing table, a label-switched interface (LSI) logical interface label is created and mapped to the VRF routing table.

Any routes present in a VRF routing table and configured with the *vrf-table-label* statement are advertised with the LSI logical interface label allocated for the VRF routing table. When packets for this VPN arrive on a core-facing interface, they are treated as if the enclosed IP packet arrived on the LSI interface and are then forwarded and filtered based on the correct table. For more information on the *vrf-table-label* statement, including a list of supported interfaces, see the *Junos VPNs Configuration Guide*.

If you configure the *family mpls* statement at the [edit interfaces interface-name unit logical-unit-number] hierarchy level and you also configure the *vrf-table-label* statement at the [edit routing-instances routing-instance-name] hierarchy level, the output for the
**show interface interface-name extensive** command includes the following output fields about the LSI traffic statistics:

- **Input bytes**—Number of bytes entering the LSI and the current throughput rate in bits per second (bps).
- **Input packets**—Number of packets entering the LSI and the current throughput rate in packets per second (pps).

---

**NOTE:** If LSI interfaces are used with VPLS when no-tunnel-services is configured or L3VPN when vrf-table-label configuration is applied inside the routing-instance, the **Input packets** field associated with the core-facing interfaces may not display the correct value. Only the Input counter is affected because the LSI is used to receive traffic from the remote PEs. Traffic that arrives on an LSI interface might not be counted at both the Traffic Statistics and the Label-switched interface (LSI) traffic statistics levels.

This note applies to the following platforms:

- M Series routers with -E3 FPC model numbers or configured with an Enhanced CFEB (CFEB-E), and M120 routers
- MX Series routers with DPC or ADPC only

The following example shows the LSI traffic statistics that you might see as part of the output of the **show interface interface-name extensive** command:

```
Label-switched interface (LSI) traffic statistics:
Input bytes:  0  0 bps
Input packets: 0 0 pps
```

### Policer Field

For the logical interface, the **Policer** field provides the policers that are to be evaluated when packets are received or transmitted on the interface. The format is **Policer: Input: type-fpc/pic/port-in-policer, Output: type-fpc/pic/port-out-policer.** For example:

```
```

### Protocol Field

For the logical interface, the **Protocol** field indicates the protocol family or families that are configured on the interface, displaying one or more of the following values:

- **aenet**—Aggregated Ethernet. Displays on Fast Ethernet interfaces that are part of an aggregated Ethernet bundle.
- **ccc**—Circuit cross-connect (CCC). Configured on the logical interface of CCC physical interfaces.
- **inet**—IP version 4 (IPv4). Configured on the logical interface for IPv4 protocol traffic, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Internet Control Message Protocol (ICMP), and Internet Protocol Control Protocol (IPCP).

- **inet6**—IP version 6 (IPv6). Configured on the logical interface for IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng), Intermediate System-to-Intermediate System (IS-IS), and BGP.

- **iso**—International Organization for Standardization (ISO). Configured on the logical interface for IS-IS traffic.

- **mlfr-uni-nni**—Multilink Frame Relay (MLFR) FRF.16 user-to-network network-to-network (UNI NNI). Configured on the logical interface for link services bundling.

- **mlfr-end-to-end**—Multilink Frame Relay end-to-end. Configured on the logical interface for multilink bundling.

- **mlppp**—Multilink Point-to-Point Protocol (MLPPP). Configured on the logical interface for multilink bundling.

- **mpls**—Multiprotocol Label Switching (MPLS). Configured on the logical interface for participation in an MPLS path.

- **pppoe**—Point-to-Point Protocol over Ethernet (PPPoE). Configured on Ethernet interfaces enabled to support multiple protocol families.

- **tcc**—Translational cross-connect (TCC). Configured on the logical interface of TCC physical interfaces.

- **tnp**—Trivial Network Protocol (TNP). Used to communicate between the Routing Engine and the router’s packet forwarding components. The Junos OS automatically configures this protocol family on the router’s internal interfaces only.

- **vpls**—Virtual private LAN service (VPLS). Configured on the logical interface on which you configure VPLS.

### RPF Failures Field

For the logical interface, the **RPF Failures** field provides information about the amount of incoming traffic (in packets and bytes) that failed a unicast reverse path forwarding (RPF) check on a particular interface. The format is **RPF Failures: Packets: xx, Bytes: yy**.

For example:

```
RPF Failures: Packets: 0, Bytes: 0
```

### Source Class Field

For the logical interface, the **Source class** field provides the names of source class usage (SCU) counters per family and per class for a particular interface. The counters display packets and bytes arriving from designated user-selected prefixes. For example:

<table>
<thead>
<tr>
<th>Source class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
</table>
Improvements to Interface Transmit Statistics Reporting

The offered load on an interface can be defined as the amount of data the interface is capable of transmitting during a given time period. The actual traffic that goes out of the interface is the transmitted load. However, when outgoing interfaces are oversubscribed, there could be traffic drops in the schedulers attached to the outgoing interfaces. Hence, the offered load is not always the same as the actual transmitted load because the offered load calculation does not take into account possible packet drop or traffic loss.

On MX Series routers, the logical interface-level statistics show the offered load, which is often different from the actual transmitted load. To address this limitation, Junos OS introduces a new configuration option in Release 11.4 R3 and later. The new configuration option, `interface-transmit-statistics`, at the `[edit interface interface-name]` hierarchy level, enables you to configure Junos OS to accurately capture and report the transmitted load on interfaces.

When the `interface-transmit-statistics` statement is included at the `[edit interface interface-name]` hierarchy level, the following operational mode commands report the actual transmitted load:

- `show interface interface-name <detail | extensive>`
- `monitor interface interface-name`
- `show snmp mib get objectID.ifIndex`

The `show interface interface-name` command also shows whether the `interface-transmit-statistics` configuration is enabled or disabled on the interface.

Related Documentation:
- `interface-transmit-statistics` on page 694
- `show interfaces` on page 1161
## show interfaces

**List of Syntax**

- Syntax (Gigabit Ethernet) on page 1161
- Syntax (10 Gigabit Ethernet) on page 1161
- Syntax (SRX Series Devices and (vSRX and vSRX 3.0 platforms)) on page 1161

### Syntax (Gigabit Ethernet)

```
show interfaces ge-fpc/pic/port 
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

### Syntax (10 Gigabit Ethernet)

```
show interfaces xe-fpc/pic/port 
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

### Syntax (SRX Series Devices and (vSRX and vSRX 3.0 platforms))

```
show interfaces ( 
   <interface-name>
   <brief | detail | extensive | terse>
   <controller interface-name>
   <descriptions interface-name>
   <destination-class (all | destination-class-name logical-interface-name)>
   <diagnostics optics interface-name>
   <far-end-interval interface-fpc/pic/port>
   <filters interface-name>
   <flow-statistics interface-name>
   <interval interface-name>
   <load-balancing (detail | interface-name)>
   <mac-database mac-address mac-address>
   <mc-ae id identifier unit number revertive-info>
   <media interface-name>
   <policers interface-name>
   <queue both-ingress-egress egress forwarding-class forwarding-class ingress l2-statistics>
   <redundancy (detail | interface-name)>
   <routing brief detail summary interface-name>
   <routing-instance (all | instance-name)>
   <snmp-index snmp-index>
   <source-class (all | destination-class-name logical-interface-name)>
   <statistics interface-name>
   <switch-port switch-port number>
   <transport pm (all | optics | otn) (all | current | currentday | interval | previousday) (all | interface-name)>
   <zone interface-name>
)
```
Release Information

Command introduced before Junos OS Release 7.4 for Gigabit interfaces.
Command introduced in Junos OS Release 8.0 for 10 Gigabit interfaces.
Command modified in Junos OS Release 9.5 for SRX Series devices.
Command introduced in Junos OS Release 18.1 for Gigabit interfaces.
Command modified in Junos OS Release 19.3R1 for MX Series Routers.

Starting in Junos OS Release 19.3R1, Output fields **ifindex** and **speed** is modified in the **show interfaces interface name extensive** command, on all MX Series routers.

- The default behavior of WAN-PHY interface remains the same. The new **precise-bandwidth** option reflects the new speed (9.294Gbps) configured on the supported line cards.
- The WAN-PHY framing mode is supported only on MPC5E and MPC6E line cards.

Command modified in Junos OS Release 19.3R1 for vSRX and vSRX 3.0 platforms to support 1G, 10G, 40G, and 100G Gigabit Ethernet interfaces, for performing CoS operations and to provide better bandwidth for processing traffic during congestion using variant speeds.

Description

Display status information about the specified Gigabit Ethernet interface.

(M320, M120, MX Series, and T Series routers only) Display status information about the specified 10-Gigabit Ethernet interface.

Display the IPv6 interface traffic statistics about the specified Gigabit Ethernet interface for MX series routers. The input and output bytes (bps) and packets (pps) rates are not displayed for IFD and local traffic.

Display status information and statistics about interfaces on SRX Series, vSRX, and vSRX 3.0 platforms running Junos OS.

**NOTE:** On SRX Series appliances, on configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

Starting in Junos OS Release 18.4R1, Output fields **Next-hop** and **vpls-status** is displayed in the **show interfaces interface name detail** command, only for Layer 2 protocols on MX480 routers.

Options

For Gigabit interfaces:

**ge-fpc/pic/port**—Display standard information about the specified Gigabit Ethernet interface.

Starting in Junos OS Release 19.3R1, on vSRX and vSRX 3.0, this interface can be configured with different speed rates of 1G, 10G, 40G, and 100G. This speed is applied for performing CoS operations and to provide better bandwidth for processing traffic during congestion.
NOTE: Interfaces with different speeds are named uniformly with `ge-0/0/x` for backward compatibility. Use the `show interfaces` command to view the interface speeds.

brief | detail | extensive | terse—(Optional) Display the specified level of output.
descriptions—(Optional) Display interface description strings.
media—(Optional) Display media-specific information about network interfaces.
snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.
statistics—(Optional) Display static interface statistics.

For 10 Gigabit interfaces:

`xe-fpc/pic/port`—Display standard information about the specified 10-Gigabit Ethernet interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.
descriptions—(Optional) Display interface description strings.
media—(Optional) Display media-specific information about network interfaces.
snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.
statistics—(Optional) Display static interface statistics.

For SRX interfaces:

- interface-name—(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number.
  - at-pim/0/port—ATM-over-ADSL or ATM-over-SHDSL interface.
  - cel-pim/0/ port—Channelized E1 interface.
  - cl-0/0/8—3G wireless modem interface for SRX320 devices.
  - ct1-pim/0/port—Channelized T1 interface.
  - dl0—Dialer Interface for initiating ISDN and USB modem connections.
  - e1-pim/0/port—E1 interface.
  - e3-pim/0/port—E3 interface.
  - fe-pim/0/port—Fast Ethernet interface.
  - ge-pim/0/port—Gigabit Ethernet interface.
Starting in Junos OS Release 19.3R1, on vSRX and vSRX 3.0, this interface supports different speed of 1G, 10G, 40G, and 100G. You can configure CoS on these interfaces. This speed is applied for performing CoS operations and to provide better bandwidth for processing traffic during congestion.

- **se-pim/0/port**—Serial interface.
- **t1-pim/0/port**—T1 (also called DS1) interface.
- **t3-pim/0/port**—T3 (also called DS3) interface.
- **wx-slot/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).
- **interface-name**—(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number.
  - **at-pim/0/port**—ATM-over-ADSL or ATM-over-SHDSL interface.
  - **cel-pim/0/port**—Channelized E1 interface.
  - **cl0/0/8**—3G wireless modem interface for SRX320 devices.
  - **ct1-pim/0/port**—Channelized T1 interface.
  - **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
  - **e1-pim/0/port**—E1 interface.
  - **e3-pim/0/port**—E3 interface.
  - **fe-pim/0/port**—Fast Ethernet interface.
  - **ge-pim/0/port**—Gigabit Ethernet interface.

Additional Information

In a logical system, this command displays information only about the logical interfaces and not about the physical interfaces.

Required Privilege

**view**
## 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, Output fields <strong>Next-hop</strong> and <strong>vpls-status</strong> is displayed in the <code>show interfaces interface name detail</code> command, only for Layer 2 protocols on MX480 routers.</td>
</tr>
</tbody>
</table>

## Related Documentation
- Understanding Layer 2 Interfaces on Security Devices
- Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration
- Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers

## List of Sample Output
- `show interfaces (Gigabit Ethernet)` on page 1203
- `show interfaces (Gigabit Ethernet on MX Series Routers)` on page 1203
- `show interfaces (link degrate status)` on page 1204
- `show interfaces extensive (Gigabit Ethernet on MX Series Routers showing interface transmit statistics configuration)` on page 1204
- `show interfaces brief (Gigabit Ethernet)` on page 1205
- `show interfaces detail (Gigabit Ethernet)` on page 1205
- `show interfaces extensive (Gigabit Ethernet IQ2)` on page 1207
- `show interfaces (Gigabit Ethernet Unnumbered Interface)` on page 1210
- `show interfaces (ACI Interface Set Configured)` on page 1210
- `show interfaces (ALI Interface Set)` on page 1211
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, IQ2)` on page 1211
- `show interfaces extensive (10-Gigabit Ethernet, WAN PHY Mode)` on page 1213
- `show interfaces extensive (10-Gigabit Ethernet, DWDM OTN PIC)` on page 1215
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode)` on page 1218
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Transmit-Only)` on page 1218
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Receive-Only)` on page 1219
- Sample Output SRX Gigabit Ethernet on page 1220
- Sample Output SRX Gigabit Ethernet on page 1221
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)` on page 1222
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)` on page 1222
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)` on page 1222
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)` on page 1222
- `show interfaces detail (Gigabit Ethernet)` on page 1223
- `show interfaces statistics st0.0 detail` on page 1224
- `show interfaces extensive (Gigabit Ethernet)` on page 1225
- `show interfaces terse on page 1228`
- `show interfaces terse (vSRX and vSRX 3.0)` on page 1229
- `show interfaces controller (Channelized E1 IQ with Logical E1)` on page 1229
- `show interfaces controller (Channelized E1 IQ with Logical DS0)` on page 1229
- `show interfaces descriptions on page 1229`
- `show interfaces destination-class all on page 1229`
show interfaces diagnostics optics on page 1230
show interfaces far-end-interval coc12-5/2/0 on page 1231
show interfaces far-end-interval coc1-5/2/1:1 on page 1231
show interfaces filters on page 1231
show interfaces flow-statistics (Gigabit Ethernet) on page 1232
show interfaces interval (Channelized OC12) on page 1233
show interfaces interval (E3) on page 1233
show interfaces interval (SONET/SDH) (SRX devices) on page 1233
show interfaces load-balancing (SRX devices) on page 1234
show interfaces load-balancing detail (SRX devices) on page 1234
show interfaces mac-database (All MAC Addresses on a Port SRX devices) on page 1234
show interfaces mac-database (All MAC Addresses on a Service SRX devices) on page 1235
show interfaces mac-database mac-address on page 1235
show interfaces mc-ae (SRX devices) on page 1236
show interfaces media (SONET/SDH) on page 1236
show interfaces policers (SRX devices) on page 1237
show interfaces policers interface-name (SRX devices) on page 1237
show interfaces queue (SRX devices) on page 1237
show interfaces redundancy (SRX devices) on page 1238
show interfaces redundancy (Aggregated Ethernet SRX devices) on page 1238
show interfaces redundancy detail (SRX devices) on page 1238
show interfaces routing brief (SRX devices) on page 1239
show interfaces routing detail (SRX devices) on page 1239
show interfaces routing-instance all (SRX devices) on page 1240
show interfaces snmp-index (SRX devices) on page 1240
show interfaces source-class all (SRX devices) on page 1240
show interfaces statistics (Fast Ethernet SRX devices) on page 1241
show interfaces switch-port (SRX devices) on page 1241
show interfaces transport pm (SRX devices) on page 1242
show security zones (SRX devices) on page 1243

Output Fields  
Table 30 on page 1166 describes the output fields for the show interfaces (Gigabit Ethernet) command. Output fields are listed in the approximate order in which they appear. For Gigabit Ethernet IQ and IQE PICs, the traffic and MAC statistics vary by interface type. For more information, see Table 31 on page 1195.

Table 30: show interfaces (Gigabit Ethernet) Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of loopback: <strong>Local</strong> or <strong>Remote</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>LAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.</td>
<td>All levels</td>
</tr>
<tr>
<td>WAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>Unidirectional link mode status for 10-Gigabit Ethernet interface: <strong>Enabled</strong> or <strong>Disabled</strong> for parent interface; <strong>Rx-only</strong> or <strong>Tx-only</strong> for child interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Remote-fault</td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Wavelength</td>
<td>(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).</td>
<td>All levels</td>
</tr>
<tr>
<td>Frequency</td>
<td>(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).</td>
<td>All levels</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedulers</td>
<td>(Gigabit Ethernet intelligent queuing 2 [IQ2] interfaces only) Number of CoS schedulers configured.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds (ms).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minutes:seconds ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps). The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Egress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for egress traffic.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Ingress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for ingress traffic.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input bytes</td>
<td>Number of bytes received on the interface. The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td>Output bytes</td>
<td>Number of bytes transmitted on the interface. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

For Gigabit Ethernet IQ PICs, the input byte counts vary by interface type. For more information, see Table 31 under the `show interfaces` command.
### Table 30: show interfaces (Gigabit Ethernet) 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>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <code>ignore-l3-incompletes</code> statement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) 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>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Due to accounting space limitations on certain Type 3 FPCs (which are supported in M320 and T640 routers), the <strong>Drops</strong> field does not always use the correct value for queue 6 or queue 7 for interfaces on 10-port 1-Gigabit Ethernet PICs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Collisions</strong>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number must always be 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field must never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Egress queues</strong></td>
<td>Total number of egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**NOTE:** In DPCs that are not of the enhanced type, such as DPC 40x1GE R, DPCE 20x1GE + 2x10GE R, or DPCE 40x1GE R, you might notice a discrepancy in the output of the `show interfaces` command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs.
### Table 30: show interfaces (Gigabit Ethernet) 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>Queue counters (Egress)</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name. Queued packets—Number of queued packets. Transmitted packets—Number of transmitted packets. Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Ingress queues</strong></td>
<td>Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Queue counters (Ingress)</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces. Queued packets—Number of queued packets. Transmitted packets—Number of transmitted packets. Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Active alarms and Active defects</strong></td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link. None—There are no active defects or alarms. Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Interface transmit statistics</strong></td>
<td>(On MX Series devices) Status of the interface-transmit-statistics configuration: Enabled or Disabled. Enabled—When the interface-transmit-statistics statement is included in the configuration. If this is configured, the interface statistics show the actual transmitted load on the interface. Disabled—When the interface-transmit-statistics statement is not included in the configuration. If this is not configured, the interface statistics show the offered load on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>OTN FEC statistics</strong></td>
<td>The forward error correction (FEC) counters provide the following statistics: Corrected Errors—Count of corrected errors in the last second. Corrected Error Ratio—Corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS statistics</td>
<td>(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Bit errors—Number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errored blocks—Number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
<tr>
<td>Link Degrade</td>
<td>Shows the link degrade status of the physical link and the estimated bit error rates (BERs). This field is available only for the PICs supporting the physical link monitoring feature.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Link Monitoring—Indicates if physical link degrade monitoring is enabled on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enable—Indicates that link downgrade monitoring has been enabled (using the link-degrade-monitor statement) on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disable—Indicates that link degrade monitoring has not been enabled on the interface. If link degrade monitoring has not been enabled, the output does not show any related information, such as BER values and thresholds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link Degrade Set Threshold—The BER threshold value at which the link is considered degraded and a corrective action is triggered.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link Degrade Clear Threshold—The BER threshold value at which the degraded link is considered recovered and the corrective action applied to the interface is reverted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Estimated BER—The estimated bit error rate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link-degrade event—Shows link degrade event information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Seconds—Time (in seconds) elapsed after a link degrade event occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—The number of link degrade events recorded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—Shows the link degrade status (example: Defect Active).</td>
<td></td>
</tr>
</tbody>
</table>
Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC statistics</td>
<td><strong>Receive and Transmit</strong> statistics reported by the PIC's MAC subsystem, including the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Total octets and total packets</strong>—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. For more information, see Table 31 under the <code>show interfaces</code> command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unicast packets, Broadcast packets, and Multicast packets</strong>—Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC/Align errors</strong>—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO error</strong>—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC control frames</strong>—Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC pause frames</strong>—Number of MAC control frames with pause operational code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Oversized frames</strong>—There are two possible conditions regarding the number of oversized frames:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet length exceeds interface MTU, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet length exceeds MRU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Jabber frames</strong>—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fragment frames</strong>—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN tagged frames</strong>—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The 20-port Gigabit Ethernet MIC (MIC-3D-20GE-SFP) does not have hardware counters for VLAN frames. Therefore, the VLAN tagged frames field displays 0 when the <code>show interfaces</code> command is executed on a 20-port Gigabit Ethernet MIC. In other words, the number of VLAN tagged frames cannot be determined for the 20-port Gigabit Ethernet MIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Code violations</strong>—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”</td>
<td></td>
</tr>
</tbody>
</table>

| OTN Received Overhead Bytes | APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08 | extensive |
| OTN Transmitted Overhead Bytes | APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08 | extensive |
Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter statistics</td>
<td><strong>Receive</strong> and <strong>Transmit</strong> statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet may enter the system or be rejected.</td>
<td></td>
</tr>
</tbody>
</table>

  - **Input packet count**—Number of packets received from the MAC hardware that the filter processed.
  - **Input packet rejects**—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.
  - **Input DA rejects**—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the router from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local router (which the router is rejecting).
  - **Input SA rejects**—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field must increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.
  - **Output packet count**—Number of packets that the filter has given to the MAC hardware.
  - **Output packet pad count**—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.
  - **Output packet error count**—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field must not increment.
  - **CAM destination filters, CAM source filters**—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields must be 0.

<table>
<thead>
<tr>
<th>PMA PHY</th>
<th>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</th>
<th>extensive</th>
</tr>
</thead>
</table>

  - **Seconds**—Number of seconds the defect has been active.
  - **Count**—Number of times that the defect has gone from inactive to active.
  - **State**—State of the error. Any state other than **OK** indicates a problem. Subfields are:
    - **PHY Lock**—Phase-locked loop
    - **PHY Light**—Loss of optical signal
### Table 30: show interfaces (Gigabit Ethernet) 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>WIS section</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B1</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOL</strong>—Loss of light</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-S</strong>—Errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-S</strong>—Severely errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEFS-S</strong>—Severely errored framing seconds (section)</td>
<td></td>
</tr>
<tr>
<td><strong>WIS line</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B2</strong>—Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-L</strong>—Remote error indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-L</strong>—Remote defect indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-L</strong>—Alarm indication signal (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-L</strong>—Errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-L</strong>—Severely errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-L</strong>—Unavailable seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-LFE</strong>—Errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-LFE</strong>—Severely errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-LFE</strong>—Unavailable seconds (far-end line)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) 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>WIS path</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B3</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-P</strong>—Remote error indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOP-P</strong>—Loss of pointer (path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-P</strong>—Path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-P</strong>—Path remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UNEQ-P</strong>—Path unequipped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLM-P</strong>—Path payload (signal) label mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-P</strong>—Errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-P</strong>—Severely errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-P</strong>—Unavailable seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-PFE</strong>—Severely errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-PFE</strong>—Unavailable seconds (far-end STS path)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation information</td>
<td>Information about link autonegotiation.</td>
<td>extensive</td>
</tr>
<tr>
<td>• Negotiation status:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Incomplete—Ethernet interface has the speed or link mode configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No autonegotiation—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Complete—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Link partner status—OK when Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Link partner—Information from the remote Ethernet device:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Link mode—Depending on the capability of the link partner, either Full-duplex or Half-duplex.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Flow control—Types of flow control supported by the link partner. For Gigabit Ethernet interfaces, types are Symmetric (link partner supports PAUSE on receive and transmit), Asymmetric (link partner supports PAUSE on transmit), Symmetric/Asymmetric (link partner supports PAUSE on receive and transmit or only PAUSE on transmit), and None (link partner does not support flow control).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote fault—Remote fault information from the link partner—Failure indicates a receive link error. OK indicates that the link partner is receiving. Negotiation error indicates a negotiation error. Offline indicates that the link partner is going offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Local resolution—Information from the local Ethernet device:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Flow control—Types of flow control supported by the local device. For Gigabit Ethernet interfaces, advertised capabilities are Symmetric/Asymmetric (local device supports PAUSE on receive and transmit or only PAUSE on receive) and None (local device does not support flow control). Depending on the result of the negotiation with the link partner, local resolution flow control type will display Symmetric (local device supports PAUSE on receive and transmit), Asymmetric (local device supports PAUSE on receive), and None (local device does not support flow control).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remote fault—Remote fault information. Link OK (no error detected on receive), Offline (local interface is offline), and Link Failure (link error detected on receive).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Received path trace, Transmitted path trace**

(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the router at the other end of the fiber. The transmitted path trace value is the message that this router transmits.

**Packet Forwarding Engine configuration**

Information about the configuration of the Packet Forwarding Engine:

• Destination slot—FPC slot number.
### Table 30: show interfaces (Gigabit Ethernet) 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>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>CoS transmit queue</strong> — Queue number and its associated user-configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td>forward class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth %</strong> — Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth bps</strong> — Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer %</strong> — Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer usec</strong> — Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Priority</strong> — Queue priority: <strong>low</strong> or <strong>high</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Limit</strong> — Displayed if rate limiting is configured for the queue. Possible values are <strong>none</strong> and <strong>exact</strong>. If <strong>exact</strong> is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If <strong>none</strong> is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

### Logical Interface

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Index</strong></td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) 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-Tag</td>
<td>Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop—The outer VLAN tag of the incoming frame is removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap—The outer VLAN tag of the incoming frame is overwritten with the user-specified VLAN tag information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• push-push—Two VLAN tags are pushed in from the incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap-push—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap-swap—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user-specified VLAN tag value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop-swap—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop-pop—Both the outer and inner VLAN tags of the incoming frame are removed.</td>
<td></td>
</tr>
<tr>
<td>Demux</td>
<td>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Source Family Inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Destination Family Inet</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>ACI VLAN</td>
<td>Information displayed for agent circuit identifier (ACI) interface set configured with the agent-circuit-id autoconfiguration stanza.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td><strong>Dynamic Profile</strong>—Name of the dynamic profile that defines the ACI interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If configured, the ACI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ACI information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The ACI VLAN field is replaced with the Line Identity field when an ALI interface set is configured with the line-identity autoconfiguration stanza.</td>
<td></td>
</tr>
<tr>
<td>Line Identity</td>
<td>Information displayed for access-line-identifier (ALI) interface sets configured with the line-identity autoconfiguration stanza.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic Profile</strong>—Name of the dynamic profile that defines the ALI interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Trusted option used to create the ALI interface set: Circuit-id, Remote-id, or Accept-no-ids. More than one option can be configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If configured, the ALI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ALI information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Line Identity field is replaced with the ACI VLAN field when an ACI interface set is configured with the agent-circuit-id autoconfiguration stanza.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 30: `show interfaces (Gigabit Ethernet)` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol family. Possible values are described in the “Protocol Field” section</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Neighbor Discovery Protocol (NDP) Queue Statistics</td>
<td>NDP statistics for protocol inet6 under logical interface statistics.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Max nh cache—Maximum interface neighbor discovery nexthop cache size.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• New hold nh limit—Maximum number of new unresolved nexthops.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Curr nh cnt—Current number of resolved nexthops in the NDP queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Curr new hold cnt—Current number of unresolved nexthops in the NDP queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NH drop cnt—Number of NDP requests not serviced.</td>
<td></td>
</tr>
<tr>
<td>Dynamic Profile</td>
<td>Name of the dynamic profile that was used to create this interface configured with</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>a Point-to-Point Protocol over Ethernet (PPPoE) family.</td>
<td></td>
</tr>
<tr>
<td>Service Name Table</td>
<td>Name of the service name table for the interface configured with a PPPoE family.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>Maximum number of PPPoE logical interfaces that can be activated on the</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>underlying interface.</td>
<td></td>
</tr>
<tr>
<td>Duplicate Protection</td>
<td>State of PPPoE duplicate protection: On or Off. When duplicate protection is</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>configured for the underlying interface, a dynamic PPPoE logical interface cannot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>be activated when an existing active logical interface is present for the same</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPPoE client.</td>
<td></td>
</tr>
<tr>
<td>Direct Connect</td>
<td>State of the configuration to ignore DSL Forum VSAs: On or Off. When configured,</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>the router ignores any of these VSAs received from a directly connected CPE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device on the interface.</td>
<td></td>
</tr>
<tr>
<td>AC Name</td>
<td>Name of the access concentrator.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Maximum labels</td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>logical interface.</td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the specified</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes, Output bytes—Number of bytes received and transmitted on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface set. The value in this field also includes the Layer 2 overhead bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for ingress or egress traffic on Ethernet interfaces if you enable accounting of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets, Output packets—Number of packets received and transmitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the interface set.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>interface if IPv6 statistics tracking is enabled.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Number and rate of bytes and packets destined to the router.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 30: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the <strong>Output bytes</strong> and <strong>Output packets</strong> interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.</td>
<td></td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the &quot;Family Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Donor interface</td>
<td>(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Preferred source address</td>
<td>(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mac-Validate Failures</td>
<td>Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the &quot;Addresses Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the address flag. Possible values are described in the &quot;Addresses Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
The following table describes the output fields for the `show interfaces (10-Gigabit Ethernet)` command.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of loopback: <strong>Local</strong> or <strong>Remote</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>LAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.</td>
<td>All levels</td>
</tr>
<tr>
<td>WAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>Unidirectional link mode status for 10-Gigabit Ethernet interface: <strong>Enabled</strong> or <strong>Disabled</strong> for parent interface; <strong>Rx-only</strong> or <strong>Tx-only</strong> for child interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Remote-fault

(Gigabit Ethernet interfaces) Remote fault status:

- **Online**—Autonegotiation is manually configured as online.
- **Offline**—Autonegotiation is manually configured as offline.

### Device flags

Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.

### Interface flags

Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.

### Link flags

Information about the link. Possible values are described in the “Links Flags” section under “Common Output Fields Description” on page 1152.

### Wavelength

(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).

### Frequency

(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).

### CoS queues

Number of CoS queues configured.

### Schedulers

(Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces only) Number of CoS schedulers configured.

### Hold-times

Current interface hold-time up and hold-time down, in milliseconds.

### Current address

Configured MAC address.

### Hardware address

Hardware MAC address.

### Last flapped

Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).

### Input Rate

Input rate in bits per second (bps) and packets per second (pps). The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.

### Output Rate

Output rate in bps and pps. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.

### Statistics last cleared

Time when the statistics for the interface were last set to zero.

### Egress account overhead

Layer 2 overhead in bytes that is accounted in the interface statistics for egress traffic.

### Ingress account overhead

Layer 2 overhead in bytes that is accounted in the interface statistics for ingress traffic.
<table>
<thead>
<tr>
<th>Traffic statistics</th>
<th>Number and rate of bytes and packets received and transmitted on the physical interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Input bytes</td>
<td>Number of bytes received on the interface. The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
</tr>
<tr>
<td>• Output bytes</td>
<td>Number of bytes transmitted on the interface. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
</tr>
<tr>
<td>• Input packets</td>
<td>Number of packets received on the interface.</td>
</tr>
<tr>
<td>• Output packets</td>
<td>Number of packets transmitted on the interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Input errors</th>
<th>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Errors</td>
<td>Sum of the incoming frame aborts and FCS errors.</td>
</tr>
<tr>
<td>• Drops</td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
</tr>
<tr>
<td>• Framing errors</td>
<td>Number of packets received with an invalid frame checksum (FCS).</td>
</tr>
<tr>
<td>• Runts</td>
<td>Number of frames received that are smaller than the runt threshold.</td>
</tr>
<tr>
<td>• Policed discards</td>
<td>Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
</tr>
<tr>
<td>• L3 incompletes</td>
<td>Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <code>ignore-l3-incompletes</code> statement.</td>
</tr>
<tr>
<td>• L2 channel errors</td>
<td>Number of times the software did not find a valid logical interface for an incoming frame.</td>
</tr>
<tr>
<td>• L2 mismatch timeouts</td>
<td>Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
</tr>
<tr>
<td>• FIFO errors</td>
<td>Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
</tr>
<tr>
<td>• Resource errors</td>
<td>Sum of transmit drops.</td>
</tr>
</tbody>
</table>
Output errors

Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:

- **Carrier transitions**—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.
- **Errors**—Sum of the outgoing frame aborts and FCS errors.
- **Drops**—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.
- **Collisions**—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.
- **Aged packets**—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.
- **FIFO errors**—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.
- **HS link CRC errors**—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.
- **MTU errors**—Number of packets whose size exceeded the MTU of the interface.
- **Resource errors**—Sum of transmit drops.

Egress queues

Total number of egress queues supported on the specified interface.

NOTE: In DPCs that are not of the enhanced type, such as DPC 40x1GE R, DPCE 20x1GE + 2x10GE R, or DPCE 40x1GE R, you might notice a discrepancy in the output of the `show interfaces` command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs.

Queue counters (Egress)

CoS queue number and its associated user-configured forwarding class name.

- **Queued packets**—Number of queued packets.
- **Transmitted packets**—Number of transmitted packets.
- **Dropped packets**—Number of packets dropped by the ASIC’s RED mechanism.

Ingress queues

Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.
<table>
<thead>
<tr>
<th>Queue counters (Ingress)</th>
<th>CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces.</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Queued packets</td>
<td>Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td>• Transmitted packets</td>
<td>Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td>• Dropped packets</td>
<td>Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
</tbody>
</table>

| Active alarms and Active defects | Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the routing device configuration, an alarm can ring the red or yellow alarm bell on the routing device, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link. |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------|----------|
| • None                            | There are no active defects or alarms.                                                                            |          |
| • Link                            | Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning. |          |

| OTN alarms | Active OTN alarms identified on the interface. | detail extensive |
| OTN defects | OTN defects received on the interface. | detail extensive |

<table>
<thead>
<tr>
<th>OTN FEC Mode</th>
<th>The FEC mode configured on the interface.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• efec</td>
<td>Enhanced forward error correction (EFEC) is configured to detect and correct bit errors.</td>
<td></td>
</tr>
<tr>
<td>• gfec</td>
<td>G.709 Forward error correction (GFEC) mode is configured to detect and correct bit errors.</td>
<td></td>
</tr>
<tr>
<td>• none</td>
<td>FEC mode is not configured.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OTN Rate</th>
<th>OTN mode.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• fixed-stuff-bytes</td>
<td>Fixed stuff bytes 11.0957 Gbps.</td>
<td></td>
</tr>
<tr>
<td>• no-fixed-stuff-bytes</td>
<td>No fixed stuff bytes 11.0491 Gbps.</td>
<td></td>
</tr>
<tr>
<td>• pass-through</td>
<td>Enable OTN passthrough mode.</td>
<td></td>
</tr>
<tr>
<td>• no-pass-through</td>
<td>Do not enable OTN passthrough mode.</td>
<td></td>
</tr>
</tbody>
</table>

| OTN Line Loopback | Status of the line loopback, if configured for the DWDM OTN PIC. Its value can be: enabled or disabled. | detail extensive |

<table>
<thead>
<tr>
<th>OTN FEC statistics</th>
<th>The forward error correction (FEC) counters for the DWDM OTN PIC.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Corrected Errors</td>
<td>The count of corrected errors in the last second.</td>
<td></td>
</tr>
<tr>
<td>• Corrected Error Ratio</td>
<td>The corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OTN FEC alarms</th>
<th>OTN FEC excessive or degraded error alarms triggered on the interface.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FEC Degrade</td>
<td>OTU FEC Degrade defect.</td>
<td></td>
</tr>
<tr>
<td>• FEC Excessive</td>
<td>OTU FEC Excessive Error defect.</td>
<td></td>
</tr>
</tbody>
</table>
**OTN OC**

OTN OC defects triggered on the interface.

- **LOS**—OC Loss of Signal defect.
- **LOF**—OC Loss of Frame defect.
- **LOM**—OC Loss of Multiframe defect.
- **Wavelength Lock**—OC Wavelength Lock defect.

**OTN OTU**

OTN OTU defects detected on the interface

- **AIS**—OTN AIS alarm.
- **BDI**—OTN OTU BDI alarm.
- **IAE**—OTN OTU IAE alarm.
- **TTIM**—OTN OTU TTIM alarm.
- **SF**—OTN ODU bit error rate fault alarm.
- **SD**—OTN ODU bit error rate defect alarm.
- **TCA-ES**—OTN ODU ES threshold alarm.
- **TCA-SES**—OTN ODU SES threshold alarm.
- **TCA-UAS**—OTN ODU UAS threshold alarm.
- **TCA-BBE**—OTN ODU BBE threshold alarm.
- **BIP**—OTN ODU BIP threshold alarm.
- **BBE**—OTN OTU BBE threshold alarm.
- **ES**—OTN OTU ES threshold alarm.
- **SES**—OTN OTU SES threshold alarm.
- **UAS**—OTN OTU UAS threshold alarm.

**Received DAPI**

Destination Access Port Interface (DAPI) from which the packets were received.

**Received SAPI**

Source Access Port Interface (SAPI) from which the packets were received.

**Transmitted DAPI**

Destination Access Port Interface (DAPI) to which the packets were transmitted.

**Transmitted SAPI**

Source Access Port Interface (SAPI) to which the packets were transmitted.

**PCS statistics**

(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.

- **Bit errors**—The number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.
- **Errored blocks**—The number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.
### MAC statistics

**Receive and Transmit** statistics reported by the PIC’s MAC subsystem, including the following:

- **Total octets and total packets**—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type.
- **Unicast packets, Broadcast packets, and Multicast packets**—Number of unicast, broadcast, and multicast packets.
- **CRC/Align errors**—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
- **FIFO error**—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.
- **MAC control frames**—Number of MAC control frames.
- **MAC pause frames**—Number of MAC control frames with pause operational code.
- **Oversized frames**—Number of frames that exceed 1518 octets.
- **Jabber frames**—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.
- **Fragment frames**—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.
- **VLAN tagged frames**—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.
- **Code violations**—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”

### OTN Received

| Overhead Bytes | APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08 | extensive |

### OTN Transmitted

| Overhead Bytes | APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08 | extensive |
Filter statistics

Receive and Transmit statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet should enter the system or be rejected.

- **Input packet count**—Number of packets received from the MAC hardware that the filter processed.
- **Input packet rejects**—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.
- **Input DA rejects**—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the routing device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local routing device (which the routing device is rejecting).
- **Input SA rejects**—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.
- **Output packet count**—Number of packets that the filter has given to the MAC hardware.
- **Output packet pad count**—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.
- **Output packet error count**—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.
- **CAM destination filters, CAM source filters**—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0.

<table>
<thead>
<tr>
<th>PMA PHY</th>
<th>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Extensive</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Seconds</strong>—Number of seconds the defect has been active.</td>
</tr>
<tr>
<td></td>
<td><strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
</tr>
<tr>
<td></td>
<td><strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
</tr>
</tbody>
</table>
### WIS section

(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:

- **Seconds**—Number of seconds the defect has been active.
- **Count**—Number of times that the defect has gone from inactive to active.
- **State**—State of the error. Any state other than **OK** indicates a problem.

Subfields are:

- **BIP-B1**—Bit interleaved parity for SONET section overhead
- **SEF**—Severely errored framing
- **LOL**—Loss of light
- **LOF**—Loss of frame
- **ES-S**—Errored seconds (section)
- **SES-S**—Severely errored seconds (section)
- **SEFS-S**—Severely errored framing seconds (section)

### WIS line

(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.

- **Seconds**—Number of seconds the defect has been active.
- **Count**—Number of times that the defect has gone from inactive to active.
- **State**—State of the error. State other than **OK** indicates a problem.

Subfields are:

- **BIP-B2**—Bit interleaved parity for SONET line overhead
- **REI-L**—Remote error indication (near-end line)
- **RDI-L**—Remote defect indication (near-end line)
- **AIS-L**—Alarm indication signal (near-end line)
- **BERR-SF**—Bit error rate fault (signal failure)
- **BERR-SD**—Bit error rate defect (signal degradation)
- **ES-L**—Errored seconds (near-end line)
- **SES-L**—Severely errored seconds (near-end line)
- **UAS-L**—Unavailable seconds (near-end line)
- **ES-LFE**—Errored seconds (far-end line)
- **SES-LFE**—Severely errored seconds (far-end line)
- **UAS-LFE**—Unavailable seconds (far-end line)
active alarms and defects, plus counts of specific SONET errors with detailed information.

- **Seconds**—Number of seconds the defect has been active.
- **Count**—Number of times that the defect has gone from inactive to active.
- **State**—State of the error. Any state other than **OK** indicates a problem.

Subfields are:

- **BIP-B3**—Bit interleaved parity for SONET section overhead
- **REI-P**—Remote error indication
- **LOP-P**—Loss of pointer (path)
- **AIS-P**—Path alarm indication signal
- **RDI-P**—Path remote defect indication
- **UNEQ-P**—Path unequipped
- **PLM-P**—Path payload label mismatch
- **ES-P**—Errored seconds (near-end STS path)
- **SES-P**—Severely errored seconds (near-end STS path)
- **UAS-P**—Unavailable seconds (near-end STS path)
- **SES-PFE**—Severely errored seconds (far-end STS path)
- **UAS-PFE**—Unavailable seconds (far-end STS path)

### Autonegotiation information

Information about link autonegotiation.

- **Negotiation status:**
  - **Incomplete**—Ethernet interface has the speed or link mode configured.
  - **No autonegotiation**—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.
  - **Complete**—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.

- **Link partner status**—**OK** when Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.

- **Link partner:**
  - **Link mode**—Depending on the capability of the attached Ethernet device, either **Full-duplex** or **Half-duplex**.
  - **Flow control**—Types of flow control supported by the remote Ethernet device. For Fast Ethernet interfaces, the type is **None**. For Gigabit Ethernet interfaces, types are **Symmetric** (link partner supports **PAUSE** on receive and transmit), **Asymmetric** (link partner supports **PAUSE** on transmit), and **Symmetric/Asymmetric** (link partner supports both **PAUSE** on receive and transmit or only **PAUSE** receive).
  - **Remote fault**—Remote fault information from the link partner—**Failure** indicates a receive link error, **OK** indicates that the link partner is receiving. **Negotiation error** indicates a negotiation error. **Offline** indicates that the link partner is going offline.

- **Local resolution**—Information from the link partner:
  - **Flow control**—Types of flow control supported by the remote Ethernet device. For Gigabit Ethernet interfaces, types are **Symmetric** (link partner supports **PAUSE** on receive and transmit), **Asymmetric** (link partner supports **PAUSE** on transmit), and **Symmetric/Asymmetric** (link partner supports both **PAUSE** on receive and transmit or only **PAUSE** receive).
  - **Remote fault**—Remote fault information. **Link OK** (no error detected on receive), **Offline** (local interface is offline), and **Link Failure** (link error detected on receive).
(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.

<table>
<thead>
<tr>
<th>Received path trace, Transmitted path trace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
</tr>
<tr>
<td>• Destination slot—FPC slot number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CoS information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about the CoS queue for the physical interface.</td>
</tr>
<tr>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding class name.</td>
</tr>
<tr>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
</tr>
<tr>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
</tr>
<tr>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
</tr>
<tr>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
</tr>
<tr>
<td>• Priority—Queue priority: low or high.</td>
</tr>
<tr>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logical Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
</tr>
<tr>
<td>Index</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
</tr>
<tr>
<td>Generation</td>
</tr>
<tr>
<td>Flags</td>
</tr>
<tr>
<td><strong>VLAN-Tag</strong></td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>push</td>
</tr>
<tr>
<td>pop</td>
</tr>
<tr>
<td>swap</td>
</tr>
<tr>
<td>push</td>
</tr>
<tr>
<td>push-push</td>
</tr>
<tr>
<td>swap-push</td>
</tr>
<tr>
<td>swap-swap</td>
</tr>
<tr>
<td>pop-swap</td>
</tr>
<tr>
<td>pop-pop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Demux:</strong></th>
<th>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</th>
<th>detail extensive none</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source Family Inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination Family Inet</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Encapsulation</strong></th>
<th>Encapsulation on the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Protocol</strong></th>
<th>Protocol family. Possible values are described in the “Protocol Field” section under “Common Output Fields Description” on page 1152.</th>
<th>detail extensive none</th>
</tr>
</thead>
</table>

| **MTU** | Maximum transmission unit size on the logical interface. | detail extensive none |

| **Maximum labels** | Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface. | detail extensive none |

<table>
<thead>
<tr>
<th><strong>Traffic statistics</strong></th>
<th>Number and rate of bytes and packets received and transmitted on the specified interface set.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Input bytes, Output bytes—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Input packets, Output packets—Number of packets received and transmitted on the interface set.</td>
<td></td>
</tr>
</tbody>
</table>

| **IPv6 transit statistics** | Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled. | extensive |

| **Local statistics** | Number and rate of bytes and packets destined to the routing device. | extensive |
**Transit statistics**  Number and rate of bytes and packets transiting the switch.

**NOTE:** For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the *Output bytes* and *Output packets* interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.

| **Generation** | Unique number for use by Juniper Networks technical support only. | detail extensive |
| **Route Table** | Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0. | detail extensive none |
| **Flags** | Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152. | detail extensive |
| **Donor interface** | (Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address. | detail extensive none |
| **Preferred source address** | (Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface. | detail extensive none |
| **Input Filters** | Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces. | detail extensive |
| **Output Filters** | Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces. | detail extensive |
| **Mac-Validate Failures** | Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface. | detail extensive none |
| **Addresses, Flags** | Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152. | detail extensive none |
| **protocol-family** | Protocol family configured on the logical interface. If the protocol is *inet*, the IP address of the interface is also displayed. | brief |
| **Flags** | Information about address flag (possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152. | detail extensive none |
| **Destination** | IP address of the remote side of the connection. | detail extensive none |
| **Local** | IP address of the logical interface. | detail extensive none |
| **Broadcast** | Broadcast address of the logical interface. | detail extensive none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | detail extensive |
For Gigabit Ethernet IQ PICs, traffic and MAC statistics output varies. The following table describes the traffic and MAC statistics for two sample interfaces, each of which is sending traffic in packets of 500 bytes (including 478 bytes for the Layer 3 packet, 18 bytes for the Layer 2 VLAN traffic header, and 4 bytes for cyclic redundancy check [CRC] information). The ge-0/3/0 interface is the inbound physical interface, and the ge-0/0/0 interface is the outbound physical interface. On both interfaces, traffic is carried on logical unit .50 (VLAN 50).

Table 31: Gigabit and 10 Gigabit Ethernet IQ PIC Traffic and MAC Statistics by Interface Type

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Sample Command</th>
<th>Byte and Octet Counts Include</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound physical interface</td>
<td>show interfaces ge-0/3/0 extensive</td>
<td>Traffic statistics:</td>
<td>The additional 4 bytes are for the CRC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 496 bytes per packet, representing the Layer 2 packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Received octets: 500 bytes per packet, representing the Layer 2 packet + 4 bytes</td>
<td></td>
</tr>
<tr>
<td>Inbound logical interface</td>
<td>show interfaces ge-0/3/0.50 extensive</td>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
<tr>
<td>Outbound physical interface</td>
<td>show interfaces ge-0/0/0 extensive</td>
<td>Traffic statistics:</td>
<td>For input bytes, the additional 12 bytes include 6 bytes for the destination MAC address plus 4 bytes for VLAN plus 2 bytes for the Ethernet type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 490 bytes per packet, representing the Layer 3 packet + 12 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Received octets: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
<tr>
<td>Outbound logical interface</td>
<td>show interfaces ge-0/0/0.50 extensive</td>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
</tbody>
</table>

Table 32 on page 1196 lists the output fields for the show interfaces command. Output fields are listed in the approximate order in which they appear.
### Table 32: show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link mode</td>
<td>Link mode: Full-duplex or Half-duplex.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>BPDU error</td>
<td>Bridge protocol data unit (BPDU) error: Detected or None</td>
<td></td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: Enabled or Disabled. If loopback is enabled, type of loopback: Local or Remote.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Remote-fault</td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Online—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Offline—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the physical link.</td>
<td>All levels</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
### Table 32: show 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>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: <em>year-month-day hour:minute:second:timezone (hour:minute:second ago).</em> For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td><strong>detail extensive</strong> none</td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps.</td>
<td>None</td>
</tr>
<tr>
<td>Active alarms and</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. These fields can contain the value None or Link.</td>
<td><strong>detail extensive</strong> none</td>
</tr>
<tr>
<td>Active defects</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>None</strong>—There are no active defects or alarms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Link</strong>—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>Statistics last</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td>cleared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 32: show 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><strong>Input errors</strong></td>
<td>Input errors on the interface.</td>
<td>Extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompleteds</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incompelt errors can be ignored by configuring the <code>ignore-l3-incompletes</code> .</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface.</td>
<td>Extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Collisions</strong>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation; therefore, for Gigabit Ethernet PICs, this number must always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field must never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 32: `show 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><strong>Ingress queues</strong></td>
<td>Total number of ingress queues supported on the specified interface.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Queue counters and queue number</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>- Queued packets</td>
<td>Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td>- Transmitted packets</td>
<td>Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td>- Dropped packets</td>
<td>Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>MAC statistics</strong></td>
<td>Receive and Transmit statistics reported by the PIC’s MAC subsystem, including the following:</td>
<td>extensive</td>
</tr>
<tr>
<td>- Total octets and total packets</td>
<td>Total number of octets and packets.</td>
<td></td>
</tr>
<tr>
<td>- Unicast packets, Broadcast packets, and Multicast packets</td>
<td>Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td>- CRC/Align errors</td>
<td>Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td>- FIFO error</td>
<td>Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>- MAC control frames</td>
<td>Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td>- MAC pause frames</td>
<td>Number of MAC control frames with pause operational code.</td>
<td></td>
</tr>
<tr>
<td>- Oversized frames</td>
<td>There are two possible conditions regarding the number of oversized frames:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Packet length exceeds 1518 octets, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Packet length exceeds MRU</td>
<td></td>
</tr>
<tr>
<td>- Jabber frames</td>
<td>Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td>- Fragment frames</td>
<td>Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runs (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td>- VLAN tagged frames</td>
<td>Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</td>
<td></td>
</tr>
<tr>
<td>- Code violations</td>
<td>Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”</td>
<td></td>
</tr>
</tbody>
</table>
### Table 32: show 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>Filter statistics</td>
<td><strong>Receive</strong> and <strong>Transmit</strong> statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet count</strong>—Number of packets received from the MAC hardware that the filter processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet rejects</strong>—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input DA rejects</strong>—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local device (which the router is rejecting).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input SA rejects</strong>—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet count</strong>—Number of packets that the filter has given to the MAC hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet pad count</strong>—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet error count</strong>—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CAM destination filters, CAM source filters</strong>—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields must be 0.</td>
<td></td>
</tr>
<tr>
<td>Autonegotiation information</td>
<td>Information about link autonegotiation.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Negotiation status:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Incomplete</strong>—Ethernet interface has the speed or link mode configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>No autonegotiation</strong>—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong>—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding Engine configuration</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination slot</strong>—FPC slot number.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 32: show 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>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>are none and exact. If exact is configured, the queue transmits only up to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured bandwidth, even if excess bandwidth is available. If none is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured, the queue transmits beyond the configured bandwidth if bandwidth</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is available.</td>
<td></td>
</tr>
<tr>
<td>Interface transmit</td>
<td>Status of the interface-transmit-statistics configuration: Enabled or Disabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>(Egress)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the specified</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes, Output bytes—Number of bytes received and transmitted on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value in this field also includes the Layer 2 overhead bytes for ingress or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>egress traffic on Ethernet interfaces if you enable accounting of Layer 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets, Output packets—Number of packets received and transmitted on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the interface set.</td>
<td></td>
</tr>
</tbody>
</table>
Table 32: show 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>Local statistics</td>
<td>Number and rate of bytes and packets destined to the device.</td>
<td>extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

**NOTE:** For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the *Output bytes* and *Output packets* interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.

| Security                | Security zones that interface belongs to.                                        | extensive       |
| Flow Input statistics   | Statistics on packets received by flow module.                                    | extensive       |
| Flow Output statistics  | Statistics on packets sent by flow module.                                        | extensive       |
| Flow error statistics   | Statistics on errors in the flow module.                                          | extensive       |
| (Packets dropped due to)|                                                                                   |                 |
| Protocol                | Protocol family.                                                                  | detail extensive none |
| MTU                     | Maximum transmission unit size on the logical interface.                          | detail extensive none |
| Generation              | Unique number for use by Juniper Networks technical support only.                 | detail extensive |
| Route Table             | Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0. | detail extensive none |
| Flags                   | Information about protocol family flags.                                          | detail extensive |
| Addresses, Flags        | Information about the address flags.                                              | detail extensive none |
| Destination             | IP address of the remote side of the connection.                                  | detail extensive none |
| Local                   | IP address of the logical interface.                                              | detail extensive none |
| Broadcast               | Broadcast address of the logical interface.                                       | detail extensive none |
| Generation              | Unique number for use by Juniper Networks technical support only.                 | detail extensive |

Copyright © 2019, Juniper Networks, Inc.
Sample Output Gigabit Ethernet

**show interfaces (Gigabit Ethernet)**

```
user@host> show interfaces ge-3/0/2

Physical interface: ge-3/0/2, Enabled, Physical link is Up
   Interface index: 167, SNMP ifIndex: 35
   Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
   Remote fault: Online
   Device flags : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   CoS queues : 4 supported, 4 maximum usable queues
   Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
   Last flapped : 2006-08-10 17:25:10 PDT (00:01:08 ago)
   Input rate : 0 bps (0 pps)
   Output rate : 0 bps (0 pps)
   Ingress rate at Packet Forwarding Engine : 0 bps (0 pps)
   Ingress drop rate at Packet Forwarding Engine : 0 bps (0 pps)
   Active alarms : None
   Active defects : None

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69)
   Flags: SNMP-Traps 0x4000
   VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push 0x8100.512 0x8100.513)
   Encapsulation: VLAN-CCC
   Egress account overhead: 100
   Ingress account overhead: 90
   Input packets : 0
   Output packets: 0
   Protocol ccc, MTU: 1522
   Flags: Is-Primary
```

**show interfaces (Gigabit Ethernet on MX Series Routers)**

```
user@host> show interfaces ge-2/2/2

Physical interface: ge-2/2/2, Enabled, Physical link is Up
   Interface index: 156, SNMP ifIndex: 188
   Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, MAC-REWRITE Error: None, Loopback: Disabled,
   Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
   Remote fault: Online
   Device flags : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Link flags : None
   CoS queues : 8 supported, 4 maximum usable queues
   Schedulers : 0
   Current address: 00:00:5e:00:53:c0, Hardware address: 00:00:5e:00:53:76
   Last flapped : 2008-09-05 16:44:30 PDT (3d 01:04 ago)
   Input rate : 0 bps (0 pps)
   Output rate : 0 bps (0 pps)
   Active alarms : None
   Active defects : None

Logical interface ge-2/2/2.0 (Index 82) (SNMP ifIndex 219)
   Flags: Up SNMP-Traps 0x4004000 Encapsulation: ENET2
   Input packets : 10232
   Output packets: 10294
```
The document contains information about network interfaces and their configurations. It includes details such as protocol information, MTU settings, link status, and interface statistics. Here's a summary of the information presented:

**Protocols and MTUs**
- **inet**: MTU 1500, Flags: Sendbcast-pkt-to-re
- **inet6**: MTU 1500, Max nh cache: 4, New hold nh limit: 100000, Curr nh cnt: 4, Curr new hold cnt: 0
- **multiservice**: MTU: Unlimited, Flags: Is-Primary

**Interface Status**
- **et-3/0/0**: Physical interface is Down, Enabled, Physical link is Down
- **ge-2/1/2**: Physical interface is Up, Enabled

**Statistics**
- **PCS statistics**:
  - Bit errors: 0
  - Errored blocks: 0
- **Link Degradation**:
  - Link Monitoring: Enable
  - Link Degradation Set Threshold: 1E-7
  - Link Degradation Clear Threshold: 1E-12
  - Estimated BER: 1E-7
  - Link-degrade event: 782 seconds

**Configuration**
- **show interfaces**
- **show interfaceset-3/0/0**
- **show interfaces ge-2/1/2 extensive | match "output|interface"**

The document provides a detailed view of network interface settings and their statuses, which is crucial for understanding network performance and diagnostics.
user@host> show interfaces ge-5/2/0.0 statistics detail
Logical interface ge-5/2/0.0 (Index 71) (SNMP ifIndex 573) (Generation 135)
  Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
  Egress account overhead: 100
  Ingress account overhead: 90
  Traffic statistics:
    Input  bytes  :               271524
    Output bytes  :             37769598
    Input  packets:                 3664
    Output packets:               885790
  IPv6 transit statistics:
    Input  bytes  :                   0
    Output bytes  :            16681118
    Input  packets:                   0
    Output packets:              362633
  Local statistics:
    Input  bytes  :               271524
    Output bytes  :               308560
    Input  packets:                 3664
    Output packets:                 3659
  Transit statistics:
    Input  bytes  :                    0 0 bps
    Output bytes  :             37461038 0 bps
    Input  packets:                    0 0 pps
    Output packets:               882131 0 pps
  IPv6 transit statistics:
    Input  bytes  :                   0 0 bps
    Output bytes  :            16681118 0 bps
    Input  packets:                   0 0 pps
    Output packets:              362633 0 pps

show interfaces brief (Gigabit Ethernet)

user@host> show interfaces ge-3/0/2 brief
Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None

Logical interface ge-3/0/2.0
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push 0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
    ccc

Logical interface ge-3/0/2.32767
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2

show interfaces detail (Gigabit Ethernet)

user@host> show interfaces ge-3/0/2 detail
Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Interface index: 167, SNMP ifIndex: 35, Generation: 177
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Source Filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags   : None
  CoS queues   : 4 supported, 4 maximum usable queues
  Hold-times   : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
  Last flapped : 2006-08-09 17:17:00 PDT (01:31:33 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input  bytes : 0  0 bps
    Output bytes : 0  0 bps
    Input  packets: 0  0 pps
    Output packets: 0  0 pps
  Ingress traffic statistics at Packet Forwarding Engine:
    Input  bytes : 0  0 bps
    Input  packets: 0  0 pps
    Drop   bytes : 0  0 bps
    Drop   packets: 0  0 pps
  Ingress queues: 4 supported, 4 in use
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 best-effort 0  0  0
    1 expedited-fo 0  0  0
    2 assured-forw 0  0  0
    3 network-cont 0  0  0
  Egress queues: 4 supported, 4 in use
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 best-effort 0  0  0
    1 expedited-fo 0  0  0
    2 assured-forw 0  0  0
    3 network-cont 0  0  0
  Active alarms : None
  Active defects : None

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69) (Generation 140)
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530)
  Out(swap-push 0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
  Egress account overhead: 100
  Ingress account overhead: 90
  Traffic statistics:
    Input  bytes : 0  0 bps
    Output bytes : 0  0 bps
    Input  packets: 0  0 pps
    Output packets: 0  0 pps
### Local statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

### Transit statistics:
- Input bytes: 0, 0 bps
- Output bytes: 0, 0 bps
- Input packets: 0, 0 pps
- Output packets: 0, 0 pps

Protocol ccc, MTU: 1522, Generation: 149, Route table: 0
Flags: Is-Primary

### Logical interface ge-3/0/2.32767 (Index 71) (SNMP ifIndex 70)
(Generation 139)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2

### Traffic statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

---

**show interfaces extensive (Gigabit Ethernet IQ2)**

```plaintext
user@host> show interfaces ge-7/1/3 extensive

Physical interface: ge-7/1/3, Enabled, Physical link is Up
Interface index: 170, SNMP ifIndex: 70, Generation: 171
Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4004000
Link flags : None
CoS queues : 8 supported, 4 maximum usable queues
Schedulers : 256
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:74, Hardware address: 00:00:5e:00:53:74
Statistics last cleared: Never
Traffic statistics:
- Input bytes: 38910844056, 7952 bps
- Output bytes: 7174605, 8464 bps
- Input packets: 418398473, 11pps
- Output packets: 78903, 12 pps
IPv6 transit statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0
```
Ingress traffic statistics at Packet Forwarding Engine:

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes</td>
<td>38910799145</td>
<td>7952 bps</td>
</tr>
<tr>
<td>Input packets</td>
<td>418397956</td>
<td>11 pps</td>
</tr>
<tr>
<td>Drop bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Drop packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
</tbody>
</table>

Input errors:
- Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0
- FIFO errors: 0, Resource errors: 0

Output errors:
- Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0
- FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Ingress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>418390823</td>
<td>418390823</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>7133</td>
<td>7133</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>1031</td>
<td>1031</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>77872</td>
<td>77872</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms: None

Active defects: None

MAC statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>38910844056</td>
<td>7174605</td>
</tr>
<tr>
<td>Total packets</td>
<td>418398473</td>
<td>78903</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>408021893366</td>
<td>1026</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>418398217</td>
<td>77865</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

OTN Received Overhead Bytes:

- APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58
- Payload Type: 0x08

OTN Transmitted Overhead Bytes:

- APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
- Payload Type: 0x08

Filter statistics:

- Input packet count: 418398473
- Input packet rejects: 479
Input DA rejects                       479
Input SA rejects                         0
Output packet count                                   78903
Output packet pad count                                   0
Output packet error count                                 0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: Symmetric/Asymmetric,
     Remote fault: OK
Local resolution:
  Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
  Destination slot: 7
CoS information:
  Direction : Output
  CoS transmit queue      Bandwidth  Buffer  Priority  Limit
                          %     bps     %      usec
  0 best-effort          95  95000000  95      0
  low none
  3 network-control      5   5000000  5       0
  low none
  Direction : Input
  CoS transmit queue      Bandwidth  Buffer  Priority  Limit
                          %     bps     %      usec
  0 best-effort          95  95000000  95      0
  low none
  3 network-control      5   5000000  5       0
  low none
Logical interface ge-7/1/3.0 (Index 70) (SNMP ifIndex 85) (Generation 150)
  Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes :               812400
  Output bytes :              1349206
  Input packets:                 9429
  Output packets:                9449
IPv6 transit statistics:
  Input bytes :                   0
  Output bytes :                   0
  Input packets:                   0
  Output packets:                   0
Local statistics:
  Input bytes :               812400
  Output bytes :              1349206
  Input packets:                 9429
  Output packets:                9449
Transit statistics:
  Input bytes :                   0                      7440 bps
  Output bytes :                   0                      7888 bps
  Input packets:                   0                       10 pps
  Output packets:                   0                       11 pps
IPv6 transit statistics:
  Input bytes :                   0
  Output bytes :                   0
  Input packets:                   0
  Output packets:                   0
Protocol inet, MTU: 1500, Generation: 169, Route table: 0
  Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
Input Filters: F1-ge-3/0/1.0-in, F3-ge-3/0/1.0-in
Output Filters: F2-ge-3/0/1.0-out (53)
Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 203.0.113.255,
Generation: 196
Protocol multiservice, MTU: Unlimited, Generation: 170, Route table: 0
Flags: Is-Primary
Policer: Input: __default_arp_policer__

NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface
egress statistics displayed in the `show interfaces` command output might not accurately
reflect the traffic on the wire when output shaping is applied. Traffic management output
shaping might drop packets after they are tallied by the interface counters. For detailed
information, see the description of the logical interface Transit statistics fields in
Table 30 on page 1166.

show interfaces (Gigabit Ethernet Unnumbered Interface)

user@host> show interfaces ge-3/2/0
Physical interface: ge-3/2/0, Enabled, Physical link is Up
  Interface index: 148, SNMP ifIndex: 50
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags: Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags: None
  CoS queues: 8 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:f8, Hardware address: 00:00:5e:00:53:f8
  Last flapped: 2006-10-27 04:42:23 PDT (08:01:52 ago)
  Input rate: 0 bps (0 pps)
  Output rate: 624 bps (1 pps)
  Active alarms: None
  Active defects: None

Logical interface ge-3/2/0.0 (Index 67) (SNMP ifIndex 85)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets: 0
  Output packets: 6
  Protocol inet, MTU: 1500
  Flags: Unnumbered
  Donor interface: lo0.0 (Index 64)
  Preferred source address: 203.0.113.22

show interfaces (ACI Interface Set Configured)

user@host> show interfaces ge-1/0/0.4001
Logical interface ge-1/0/0.4001 (Index 340) (SNMP ifIndex 548)
  Flags: SNMP-Traps Encapsulation: PPP-over-
  Ethernet
  ACI VLAN:
  Dynamic Profile: aci-vlan-set-profile
  PPPoE:
show interfaces (ALI Interface Set)

user@host> show interfaces ge-1/0/0.10

Logical interface ge-1/0/0.10 (Index 346) (SNMP ifIndex 554) (Generation 155)
Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.10 ] Encapsulation: ENET2

Dynamic Profile: ali-set-profile
Circuit-id Remote-id Accept-no-ids

PPPoE:
Dynamic Profile: ali-vlan-pppoe-profile,
Service Name Table: None,
Max Sessions: 32000, Max Sessions VSA Ignore: Off,
Duplicate Protection: On, Short Cycle Protection: Off,
Direct Connect: Off,
AC Name: nbc
Input packets : 9
Output packets: 8
Protocol multiservice, MTU: Unlimited

Sample Output Gigabit Ethernet

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, IQ2)

user@host> show interfaces xe-5/0/0 extensive

Physical interface: xe-5/0/0, Enabled, Physical link is Up
Interface index: 177, SNMP ifIndex: 630, Generation: 178
Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Speed: 10Gbps, Loopback:
None, Source filtering: Enabled,
Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 8 supported, 4 maximum usable queues
Schedulers : 1024
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:f6, Hardware address: 00:00:5e:00:53:f6
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 6970332384 0 bps
Output bytes : 0 0 bps
Input packets: 810506 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Ingress traffic statistics at Packet Forwarding Engine:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes</td>
<td>6970299398</td>
</tr>
<tr>
<td>Input packets</td>
<td>81049992</td>
</tr>
<tr>
<td>Drop bytes</td>
<td>0</td>
</tr>
<tr>
<td>Drop packets</td>
<td>0</td>
</tr>
</tbody>
</table>

Input errors:

- Errors: 0
- Drops: 0
- Framing errors: 0
- Runts: 0
- Policed discards: 0
- L3 incompletes: 0
- L2 channel errors: 0
- L2 mismatch timeouts: 0
- FIFO errors: 0
- Resource errors: 0

Output errors:

- Carrier transitions: 0
- Errors: 0
- Drops: 0
- Collisions: 0
- Aged packets: 0
- FIFO errors: 0
- HS link CRC errors: 0
- MTU errors: 0
- Resource errors: 0

Ingress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>81049992</td>
<td>81049992</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms: None

Active defects: None

PCS statistics

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>0</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>0</td>
</tr>
</tbody>
</table>

MAC statistics

<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>6970332384</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>81050506</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>81050000</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>506</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet count</td>
<td>81050506</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>506</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces xe-1/0/0 extensive

user@host> show interfaces xe-1/0/0 extensive

Chapter 14: Interface Operational Commands
Physical interface: xe-1/0/0, Enabled, Physical link is Up  
Interface index: 141, SNMP ifIndex: 630, Generation: 47  
Link-level type: Ethernet, MTU: 1514, Speed: 9.294Gbps  
Loopback: Disabled  
WAN-PHY mode  
Source filtering: Disabled, Flow control: Enabled  
Speed Configuration: Auto  
Device flags: Present Running  
Interface flags: SNMP-Traps 16384  
Link flags: None  
CoS queues: 4 supported  
Hold-times: Up 0 ms, Down 0 ms  
Current address: 00:00:5e:00:53:9d, Hardware address: 00:00:5e:00:53:9d  
Statistics last cleared: Never  
Traffic statistics:  
| Input bytes | 0  | 0 bps |  
| Output bytes | 0  | 0 bps |  
| Input packets | 0  | 0 pps |  
| Output packets | 0  | 0 pps |  
Input errors:  
| Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, HS Link CRC errors: 0, HS Link FIFO overflows: 0, Resource errors: 0 |  
Output errors:  
| Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0 |  
Queue counters:  
| Queued packets | Transmitted packets | Dropped packets |  
| 0 best-effort | 0 | 0 | 0 |  
| 1 expedited-forw | 0 | 0 | 0 |  
| 2 assured-forward | 0 | 0 | 0 |  
| 3 network-cont | 0 | 0 | 0 |  
Active alarms: LOL, LOS, LBL  
Active defects: LOL, LOS, LBL, SEF, AIS-L, AIS-P  
PCS statistics:  
| Seconds | Count |  
| Bit errors | 0 | 0 |  
| Errored blocks | 0 | 0 |  
MAC statistics:  
| Receive | Transmit |  
| Total octets | 0 | 0 |  
| Total packets | 0 | 0 |  
| Unicast packets | 0 | 0 |  
| Broadcast packets | 0 | 0 |  
| Multicast packets | 0 | 0 |  
| CRC/Align errors | 0 | 0 |  
| FIFO errors | 0 | 0 |  
| MAC control frames | 0 | 0 |  
| MAC pause frames | 0 | 0 |  
| Oversized frames | 0 | 0 |  
| Jabber frames | 0 | 0 |  
| Fragment frames | 0 | 0 |  
| VLAN tagged frames | 0 | 0 |  
| Code violations | 0 | 0 |  
Filter statistics:  
| Input packet count | 0 |  
| Input packet rejects | 0 |  
| Input DA rejects | 0 |  
| Input SA rejects | 0 |  
| Output packet count | 0 |  
| Output packet pad count | 0 |  

Copyright © 2019, Juniper Networks, Inc.
Output packet error count: 0
CAM destination filters: 0, CAM source filters: 0
PMA PHY:
  PLL lock: 0s 0s 0s OK
  PHY light: 63159s 1s Light Missing
WIS section:
  BIP-B1: 0 0
  SEF: 434430 434438 Defect Active
  LOS: 434430 1 Defect Active
  LOF: 434430 1 Defect Active
  ES-S: 434430
  SES-S: 434430
  SEFS-S: 434430
WIS line:
  BIP-B2: 0 0
  REI-L: 0 0
  RDI-L: 0 0 OK
  AIS-L: 434430 1 Defect Active
  BERR-SF: 0 0 OK
  BERR-SD: 0 0 OK
  ES-L: 434430
  SES-L: 434430
  UAS-L: 434420
  ES-LFE: 0
  SES-LFE: 0
  UAS-LFE: 0
WIS path:
  BIP-B3: 0 0
  REI-P: 0 0
  LOP-P: 0 0 OK
  AIS-P: 434430 1 Defect Active
  RDI-P: 0 0 OK
  UNEQ-P: 0 0 OK
  PLM-P: 0 0 OK
  ES-P: 434430
  SES-P: 434430
  UAS-P: 434420
  ES-PFE: 0
  SES-PFE: 0
  UAS-PFE: 0
Received path trace:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
Transmitted path trace: orissa so-1/0/0
  6f 72 69 73 73 61 20 73 6f 2d 31 2f 30 2f 30 00 orissa so-1/0/0.
Packet Forwarding Engine configuration:
  Destination slot: 1
CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>bps</td>
<td>%</td>
<td>bytes</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>950000000</td>
<td>95</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>500000000</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>
Flow control: Enabled  
Device flags   : Present Running Down  
Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000  
Link flags     : None  
Wavelength     : 1550.12 nm, Frequency: 193.40 THz  
CoS queues     : 8 supported, 8 maximum usable queues  
Hold-times     : Up 0 ms, Down 0 ms  
Current address: 00:00:5e:00:53:72, Hardware address: 00:00:5e:00:53:72  
Statistics last cleared: Never  
Traffic statistics:  
Input bytes : 0 0 bps  
Output bytes : 0 0 bps  
Input packets: 0 0 pps  
Output packets: 0 0 pps  
IPV6 transit statistics:  
Input bytes : 0  
Output bytes : 0  
Input packets: 0  
Output packets: 0  
Input errors:  
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,  
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,  
FIFO errors: 0, Resource errors: 0  
Output errors:  
Carrier transitions: 2, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,  
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0  
Egress queues: 8 supported, 4 in use  
Queue counters: Queued packets Transmitted packets Dropped packets  
0 best-effort 0 0 0  
1 expedited-fo 0 0 0  
2 assured-forw 0 0 0  
3 network-cont  
Queue number: Mapped forwarding classes  
0 best-effort  
1 expedited-forwarding  
2 assured-forwarding  
3 network-control  
Active alarms  : LINK  
Active defects : LINK  
MAC statistics: Receive Transmit  
Total octets 0 0  
Total packets 0 0  
Unicast packets 0 0  
Broadcast packets 0 0  
Multicast packets 0 0  
CRC/Align errors 0 0  
FIFO errors 0 0  
MAC control frames 0 0  
MAC pause frames 0 0  
Oversized frames 0 0  
Jabber frames 0 0  
Fragment frames 0 0  
VLAN tagged frames 0 0  
Code violations 0 0  
Total octets 0 0
| Total packets                      | 0   |          |
| Unicast packets                   | 0   |          |
| Broadcast packets                 | 0   |          |
| Multicast packets                 | 0   |          |
| CRC/Align errors                  | 0   |          |
| FIFO errors                       | 0   |          |
| MAC control frames                | 0   |          |
| MAC pause frames                  | 0   |          |
| Oversized frames                  | 0   |          |
| Jabber frames                     | 0   |          |
| Fragment frames                   | 0   |          |
| VLAN tagged frames                | 0   |          |
| Code violations                   | 0   |          |
| OTN alarms                        : None |
| OTN defects                       : None |
| OTN FEC Mode                      : GFEC |
| OTN Rate                          : Fixed Stuff Bytes 11.0957Gbps |
| OTN Line Loopback                 : Enabled |
| OTN FEC statistics: |
| Corrected Errors                  | 0   |
| Corrected Error Ratio             | 0e-0 |
| OTN FEC alarms: |
| FEC Degrade                       | 0   | OK       |
| FEC Excessive                     | 0   | OK       |
| OTN OC: |
| LOS                               | 2   | 1 OK     |
| LOF                               | 67164 | 2 Defect Active |
| LOM                               | 67164 | 71 Defect Active |
| Wavelength Lock                   | 0   | OK       |
| OTN OTU: |
| AIS                               | 0   | OK       |
| BDI                               | 65919 | 4814 Defect Active |
| IAE                               | 67158 | 1 Defect Active |
| TTIM                              | 7   | 1 OK     |
| SF                                | 67164 | 2 Defect Active |
| SD                                | 67164 | 3 Defect Active |
| TCA-ES                            | 0   | OK       |
| TCA-SES                           | 0   | OK       |
| TCA-UAS                           | 80  | 40 OK    |
| BIP                               | 0   | OK       |
| BBE                               | 0   | OK       |
| ES                                | 0   | OK       |
| SES                               | 0   | OK       |
| UAS                               | 587 | OK       |
| Received DAPI: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... |
| Received SAPI: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... |
| Transmitted DAPI: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... |
| Transmitted SAPI: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... |
| OTN Received Overhead Bytes: |
| APS/PCC0: 0x02, APS/PCC1: 0x42, APS/PCC2: 0xa2, APS/PCC3: 0x48 |
| Payload Type: 0x03 |
| OTN Transmitted Overhead Bytes: |
| APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 |
| Payload Type: 0x03 |
| Filter statistics: |
show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode)

```
show interfaces xe-7/0/0 extensive

Physical interface: xe-7/0/0, Enabled, Physical link is Up
  Interface index: 173, SNMP ifIndex: 212, Generation: 174
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Enabled,
  Loopback: None, Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
  Last flapped   : 2007-06-01 09:08:19 PDT (3d 02:31 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 322891152287160 9627472888 bps
    Input packets: 0 0 pps
    Output packets: 328809727380 1225492 pps
  ...
```

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Transmit-Only)

```
show interfaces xe-7/0/0–tx extensive

Physical interface: xe-7/0/0-tx, Enabled, Physical link is Up
  Interface index: 176, SNMP ifIndex: 137, Generation: 177
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Tx-Only
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
  Last flapped   : 2007-06-01 09:08:19 PDT (3d 02:31 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 322891152287160 9627472888 bps
    Input packets: 0 0 pps
    Output packets: 328809727380 1225492 pps
  ...
```
Logical interface xe-7/0/0-tx.0 (Index 73) (SNMP ifIndex 138) (Generation 139)

Flags: SNMP-Traps Encapsulation: ENET2
Egress account overhead: 100
Ingress account overhead: 90
Traffic statistics:
Input bytes : 0
Output bytes : 322891152287160
Input packets: 0
Output packets: 328809727380
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 322891152287160 9627472888 bps
Input packets: 0 0 pps
Output packets: 328809727380 1225492 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: 1500, Generation: 147, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 10.11.12/24, Local: 10.11.12.13, Broadcast: 10.11.12.255,
Generation: 141
Protocol multiservice, MTU: Unlimited, Generation: 148, Route table: 0
Flags: None
Policer: Input: __default_arp_policer__

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Receive-Only)

user@host> show interfaces xe-7/0/0-rx extensive

Physical interface: xe-7/0/0-rx, Enabled, Physical link is Up
Interface index: 174, SNMP ifIndex: 118, Generation: 175
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
Unidirectional: Rx-Only
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
Last Flapped : 2007-06-01 09:08:22 PDT (3d 02:31 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 32285746303482 9627496104 bps
Sample Output

Sample Output SRX Gigabit Ethernet

```
user@host> show interfaces ge-0/0/1

Physical interface: ge-0/0/1, Enabled, Physical link is Down
  Interface index: 135, SNMP ifIndex: 510
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
```
Sample Output SRX Gigabit Ethernet

user@host> show interfaces ge-0/0/1

Physical interface: ge-0/0/1, Enabled, Physical link is Down

Interface index: 135, SNMP ifIndex: 510
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,

BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online

Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:42 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
Active alarms : LINK
Active defects : LINK
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Input packets : 0
Output packets: 0
Security: Zone: public
Protocol inet, MTU: 1500

Flags: Sendbcast-pkt-to-re
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255
show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/0

Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 510
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Link-mode: Half-duplex,
  Speed: 1000mbps, BPDU Error: None, Loop Detect PDU Error: None, Ethernet-Switching
  Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering:
  Disabled, Flow control: Enabled,
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:ef:25, Hardware address: 00:50:56:93:ef:25
  Last flapped   : 2019-03-29 01:57:45 UTC (00:00:41 ago)
  Input rate     : 1120 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/2

Physical interface: ge-0/0/2, Enabled, Physical link is Up
  Interface index: 137, SNMP ifIndex: 525
  Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source
  filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:30:40, Hardware address: 00:50:56:93:30:40

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/3

Physical interface: ge-0/0/3, Enabled, Physical link is Up
  Interface index: 138, SNMP ifIndex: 526
  Link-level type: Ethernet, MTU: 1514, Speed: 40Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source
  filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:30:4d, Hardware address: 00:50:56:93:30:4d

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/4

Physical interface: ge-0/0/4, Enabled, Physical link is Up
  Interface index: 139, SNMP ifIndex: 527
  Link-level type: Ethernet, MTU: 1514, Speed: 100Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source
  filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
show interfaces detail (Gigabit Ethernet)

user@host> show interfaces ge-0/0/1 detail

Physical interface: ge-0/0/1, Enabled, Physical link is Down

Interface index: 135, SNMP ifIndex: 510, Generation: 138
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w2d 00:00 ago)
Statistics last cleared: Never
Traffic statistics:
 Input bytes : 0  0 bps
 Output bytes : 0  0 bps
 Input packets: 0  0 pps
 Output packets: 0  0 pps
Egress queues: 8 supported, 4 in use
Queue counters:
 0 best-effort  Queued packets  Transmitted packets  Dropped packets
 0 0 0 0
 1 expedited-fo 0 0 0
 2 assured-forw 0 0 0
 3 network-cont 0 0 0
Queue number: Mapped forwarding classes
 0 best-effort
 1 expedited-forwarding
 2 assured-forwarding
 3 network-control
Active alarms : LINK
Active defects : LINK
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
Local statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
### Transit Statistics

- **Input bytes**: 0, **0 bps**
- **Output bytes**: 0, **0 bps**
- **Input packets**: 0, **0 pps**
- **Output packets**: 0, **0 pps**

### Flow Statistics

- **Flow Input statistics**
  - **Self packets**: 0
  - **ICMP packets**: 0
  - **VPN packets**: 0
  - **Multicast packets**: 0
  - **Bytes permitted by policy**: 0
  - **Connections established**: 0

- **Flow Output statistics**
  - **Multicast packets**: 0
  - **Bytes permitted by policy**: 0

### Flow error statistics (Packets dropped due to):

- **Address spoofing**: 0
- **Authentication failed**: 0
- **Incoming NAT errors**: 0
- **Invalid zone received packet**: 0
- **Multiple user authentications**: 0
- **Multiple incoming NAT**: 0
- **No parent for a gate**: 0
- **No one interested in self packets**: 0
- **No minor session**: 0
- **No more sessions**: 0
- **No NAT gate**: 0
- **No route present**: 0
- **No SA for incoming SPI**: 0
- **No tunnel found**: 0
- **No session for a gate**: 0
- **No zone or NULL zone binding**: 0
- **Policy denied**: 0
- **Security association not active**: 0
- **TCP sequence number out of window**: 0
- **Syn-attack protection**: 0
- **User authentication errors**: 0

### Protocol inet, MTU: 1500, Generation: 150, Route table: 0

### Flags: Sendicast-pkt-to-re

- **Addresses, Flags**: Dest-route-down Is-Preferred Is-Primary
- **Destination**: 1.1.1.24, **Local**: 1.1.1.1, **Broadcast**: 1.1.1.255, **Generation**: 150

---

**show interfaces statistics st0.0 detail**

```
user@host> show interfaces statistics st0.0 detail

Logical interface st0.0 (Index 71) (SNMP ifIndex 609) (Generation 136)
  Flags: Up Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel

Traffic statistics:
- **Input bytes**: 528152756774
- **Output bytes**: 575950643520
- **Input packets**: 11481581669
- **Output packets**: 12520666095

Local statistics:
- **Input bytes**: 0
- **Output bytes**: 0
```
show interfaces extensive (Gigabit Ethernet)

user@host> show interfaces ge-0/0/1.0 extensive

  Physical interface: ge-0/0/1, Enabled, Physical link is Down
  Interface index: 135, SNMP ifIndex: 510, Generation: 138
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:57 ago)
Statistics last cleared: Never
Traffic statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Output bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Input packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>Output packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
</tbody>
</table>

Input errors:
- Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
- L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
- FIFO errors: 0, Resource errors: 0

Output errors:
- Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
- FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use
Queue counters:
<table>
<thead>
<tr>
<th>Queue number</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control

Active alarms : LINK
Active defects : LINK
MAC statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet count</td>
<td>0</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
</tbody>
</table>
Input SA rejects: 0
Output packet count: 0
Output packet pad count: 0
Output packet error count: 0
CAM destination filters: 2, CAM source filters: 0
Autonegotiation information:
   Negotiation status: Incomplete
Packet Forwarding Engine configuration:
   Destination slot: 0
CoS information:
   Direction: Output
   CoS transmit queue | Bandwidth | Buffer Priority
   Limit
   | %         | bps        | %        | usec | Priority |
   0 best-effort 95 950000000 95 0 low
   none
   3 network-control 5 50000000 5 0 low
   none
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
   Input bytes: 0
   Output bytes: 0
   Input packets: 0
   Output packets: 0
Local statistics:
   Input bytes: 0
   Output bytes: 0
   Input packets: 0
   Output packets: 0
Transit statistics:
   Input bytes: 0 0 bps
   Output bytes: 0 0 bps
   Input packets: 0 0 pps
   Output packets: 0 0 pps
Security: Zone: public
Flow Statistics:
Flow Input statistics:
   Self packets: 0
   ICMP packets: 0
   VPN packets: 0
   Multicast packets: 0
   Bytes permitted by policy: 0
   Connections established: 0
Flow Output statistics:
   Multicast packets: 0
   Bytes permitted by policy: 0
Flow error statistics (Packets dropped due to):
   Address spoofing: 0
   Authentication failed: 0
   Incoming NAT errors: 0
   Invalid zone received packet: 0
   Multiple user authentications: 0
   Multiple incoming NAT: 0
   No parent for a gate: 0
   No one interested in self packets: 0
   No minor session: 0
   No more sessions: 0
show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up inet</td>
<td>10.209.4.61/18</td>
</tr>
<tr>
<td>gr-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>ip-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>st0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>st0.1</td>
<td>up</td>
<td>ready inet</td>
<td></td>
</tr>
<tr>
<td>ls-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>lt-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>mt-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>pd-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>pe-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>e3-1/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>t3-2/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>e1-3/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>se-4/0/0</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>tl-5/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>br-6/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>dc-6/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>dc-6/0/0.32767</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>bc-6/0/0.1</td>
<td>down</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>bc-6/0/0:1.0</td>
<td>up</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>dl0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>dl0.0</td>
<td>up</td>
<td>up inet</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>dsc</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>gre</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>ipip</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>lo0.16385</td>
<td>up</td>
<td>up inet</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>lsi</td>
<td>up</td>
<td>up</td>
<td>10.0.0.16</td>
</tr>
<tr>
<td>mtun</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>pimd</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>pime</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>pp0</td>
<td>up</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>
**show interfaces terse (vSRX and vSRX 3.0)**

```plaintext
user@host> show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>1.1.65.1/24</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**show interfaces controller (Channelized E1IQ with Logical E1)**

```plaintext
user@host> show interfaces controller ce1-1/2/6

<table>
<thead>
<tr>
<th>Controller</th>
<th>Admin</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce1-1/2/6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>e1-1/2/6</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
```

**show interfaces controller (Channelized E1IQ with Logical DS0)**

```plaintext
user@host> show interfaces controller ce1-1/2/3

<table>
<thead>
<tr>
<th>Controller</th>
<th>Admin</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce1-1/2/3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ds-1/2/3:1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ds-1/2/3:2</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
```

**show interfaces descriptions**

```plaintext
user@host> show interfaces descriptions

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-1/0/0</td>
<td>up</td>
<td>up</td>
<td>M20-3#1</td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>up</td>
<td>up</td>
<td>GSR-12#1</td>
</tr>
<tr>
<td>ge-3/0/0</td>
<td>up</td>
<td>up</td>
<td>SMB-OSPF_Area300</td>
</tr>
<tr>
<td>so-3/3/0</td>
<td>up</td>
<td>up</td>
<td>GSR-13#1</td>
</tr>
<tr>
<td>so-3/3/1</td>
<td>up</td>
<td>up</td>
<td>GSR-13#2</td>
</tr>
<tr>
<td>ge-4/0/0</td>
<td>up</td>
<td>up</td>
<td>T320-7#1</td>
</tr>
<tr>
<td>ge-5/0/0</td>
<td>up</td>
<td>up</td>
<td>T320-7#2</td>
</tr>
<tr>
<td>so-7/1/0</td>
<td>up</td>
<td>up</td>
<td>M160-6#1</td>
</tr>
<tr>
<td>ge-8/0/0</td>
<td>up</td>
<td>up</td>
<td>T320-7#3</td>
</tr>
<tr>
<td>ge-9/0/0</td>
<td>up</td>
<td>up</td>
<td>T320-7#4</td>
</tr>
<tr>
<td>so-10/0/0</td>
<td>up</td>
<td>up</td>
<td>M160-6#2</td>
</tr>
<tr>
<td>so-13/0/0</td>
<td>up</td>
<td>up</td>
<td>M20-3#2</td>
</tr>
<tr>
<td>so-14/0/0</td>
<td>up</td>
<td>up</td>
<td>GSR-12#2</td>
</tr>
<tr>
<td>ge-15/0/0</td>
<td>up</td>
<td>up</td>
<td>SMB-OSPF_Area100</td>
</tr>
<tr>
<td>ge-15/0/1</td>
<td>up</td>
<td>up</td>
<td>GSR-13#3</td>
</tr>
</tbody>
</table>
```

**show interfaces destination-class all**

```plaintext
user@host> show interfaces destination-class all
```
show interfaces diagnostics optics

user@host> show interfaces diagnostics optics ge-2/0/0

Physical interface: ge-2/0/0

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser bias current</td>
<td>7.408 mA</td>
</tr>
<tr>
<td>Laser output power</td>
<td>0.3500 mW / -4.56 dBm</td>
</tr>
<tr>
<td>Module temperature</td>
<td>23 degrees C / 73 degrees F</td>
</tr>
<tr>
<td>Module voltage</td>
<td>3.3450 V</td>
</tr>
<tr>
<td>Receiver signal average optical power</td>
<td>0.0002 mW / -36.99 dBm</td>
</tr>
<tr>
<td>Laser bias current high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power low alarm</td>
<td>On</td>
</tr>
<tr>
<td>Laser rx power high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current high alarm threshold</td>
<td>17.000 mA</td>
</tr>
<tr>
<td>Laser bias current low alarm threshold</td>
<td>1.000 mA</td>
</tr>
<tr>
<td>Laser bias current high warning threshold</td>
<td>14.000 mA</td>
</tr>
<tr>
<td>Laser bias current low warning threshold</td>
<td>2.000 mA</td>
</tr>
<tr>
<td>Laser output power high alarm threshold</td>
<td>0.6310 mW / -2.00 dBm</td>
</tr>
<tr>
<td>Laser output power low alarm threshold</td>
<td>0.0670 mW / -11.74 dBm</td>
</tr>
<tr>
<td>Laser output power high warning threshold</td>
<td>0.6310 mW / -2.00 dBm</td>
</tr>
<tr>
<td>Laser output power low warning threshold</td>
<td>0.0790 mW / -11.02 dBm</td>
</tr>
<tr>
<td>Module temperature high alarm threshold</td>
<td>95 degrees C / 203 degrees F</td>
</tr>
<tr>
<td>Module temperature low alarm threshold</td>
<td>-25 degrees C / -13 degrees F</td>
</tr>
<tr>
<td>Module temperature high warning threshold</td>
<td>90 degrees C / 194 degrees F</td>
</tr>
<tr>
<td>Module temperature low warning threshold</td>
<td>-20 degrees C / -4 degrees F</td>
</tr>
<tr>
<td>Module voltage high alarm threshold</td>
<td>3.900 V</td>
</tr>
<tr>
<td>Module voltage low alarm threshold</td>
<td>2.700 V</td>
</tr>
<tr>
<td>Module voltage high warning threshold</td>
<td>3.700 V</td>
</tr>
</tbody>
</table>
show interfaces far-end-interval coc12-5/2/0

show interfaces far-end-interval coc1-5/2/1:1

show interfaces filters
show interfaces flow-statistics (Gigabit Ethernet)

user@host> show interfaces flow-statistics ge-0/0/1.0

Logical interface ge-0/0/1.0 (Index 70) (SNMP ifIndex 49)
Flags: SNMP-Traps Encapsulation: ENET2
Input packets : 5161
Output packets: 83
Security: Zone: zone2
Allowed host-inbound traffic : bootp bfd bgp dns dvmrp ldp msdp nhrp ospf
pgm
pim rip router-discovery rsvp sap vrrp finger ftp tftp ident-reset http
https ike
netconf ping rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
xnm-ssl
1sging
Flow Statistics :
Flow Input statistics :
Self packets : 0
ICMP packets : 0
VPN packets : 2564
Bytes permitted by policy : 3478
Connections established : 1
Flow Output statistics:
Multicast packets : 0
Bytes permitted by policy : 16994
Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
show interfaces interval (Channelized OC12)

user@host> show interfaces interval t3-0/3/0:0

Physical interface: t3-0/3/0:0, SNMP ifIndex: 23
17:43-current:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:28–17:43:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:13–17:28:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:58–17:13:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:43–16:58:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  ...
Interval Total:
  LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,

show interfaces interval (E3)

user@host> show interfaces interval e3-0/3/0

Physical interface: e3-0/3/0, SNMP ifIndex: 23
17:43-current:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:28–17:43:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:13–17:28:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:58–17:13:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:43–16:58:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  ...
Interval Total:
  LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,

show interfaces interval (SONET/SDH) (SRX devices)

user@host> show interfaces interval so-0/1/0
Interfaces Fundamentals for Routing Devices

Physical interface: so-0/1/0, SNMP ifIndex: 19
20:02-current:
   ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0,
   SES-P: 0, UAS-P: 0
19:47-20:02:
   ES-S: 267, SES-S: 267, SEFS-S: 267, ES-L: 267, SES-L: 267, UAS-L: 267,
   ES-P: 267, SES-P: 267, UAS-P: 267
19:32-19:47:
   ES-S: 56, SES-S: 56, SEFS-S: 56, ES-L: 56, SES-L: 56, UAS-L: 46, ES-P: 56,
   SES-P: 56, UAS-P: 46
19:17-19:32:
   ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0,
   SES-P: 0, UAS-P: 0
19:02-19:17:
   .....
show interfaces mac-database (All MAC Addresses on a Service SRX devices)

user@host> show interfaces mac-database xe-0/3/3
Logical interface xe-0/3/3 (Index 364) (SNMP ifIndex 829)
  Flags: SNMP-Traps 0x0004000 Encapsulation: ENET2
  MAC address  Input frames  Input bytes  Output frames  Output bytes
  00:00:00:00:00:00             1             56              0              0
  00:00:c0:01:01:02       7023810      323095260              0              0
  00:00:c0:01:01:03       7023810      323095260              0              0
  00:00:c0:01:01:04       7023810      323095260              0              0
  00:00:c0:01:01:05       7023810      323095260              0              0
  00:00:c0:01:01:06       7023810      323095260              0              0
  00:00:c0:01:01:07       7023810      323095260              0              0
  00:00:c0:01:01:08       7023809      323095214              0              0
  00:00:c0:01:01:09       7023809      323095214              0              0
  00:00:c0:01:01:0a       7023809      323095214              0              0
  00:00:c0:01:01:0b       7023809      323095214              0              0
  00:00:c8:01:01:02      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:03      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:04      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:05      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:06      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:07      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:08      30424784     1399540064       37448598     1722635508
  00:00:c8:01:01:09       8836796      406492616        8836795      406492570
  00:00:c8:01:01:0a      30424716     1399536936       37448523     1722632058
  00:00:c8:01:01:0b      30424716     1399536936       37448523     1722632058

Number of MAC addresses : 21

show interfaces mac-database mac-address

user@host> show interfaces mac-database xe-0/3/3 mac-address (SRX devices)
00:00:c8:01:01:09
Physical interface: xe-0/3/3, Enabled, Physical link is Up
  Interface index: 372, SNMP ifIndex: 788
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, Loopback: None, Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running

Copyright © 2019, Juniper Networks, Inc.
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None

Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
Flags: SNMP-Traps 0x40004000 Encapsulation: ENET2
MAC address: 00:00:c8:01:01:09, Type: Configured,
Input bytes : 202324652
Output bytes : 202324560
Input frames : 4398362
Output frames : 4398360
Policer statistics:
<table>
<thead>
<tr>
<th>Policer type</th>
<th>Discarded frames</th>
<th>Discarded bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output aggregate</td>
<td>3992386</td>
<td>183649756</td>
</tr>
</tbody>
</table>

show interfaces mc-ae (SRX devices)

user@host> show interfaces mc-ae ae0 unit 512
Member Links : ae0
Local Status : active
Peer Status : active
Logical Interface : ae0.512
Core Facing Interface : Label Ethernet Interface
ICL-PL : Label Ethernet Interface

show interfaces media (SONET/SDH)

The following example displays the output fields unique to the `show interfaces media` command for a SONET interface (with no level of output specified):

user@host> show interfaces media so-4/1/2
Physical interface: so-4/1/2, Enabled, Physical link is Up
Interface index: 168, SNMP ifIndex: 495
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 1783 (00:00:00 ago), Output: 1786 (00:00:08 ago)
LCP state: Opened
NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Not-configured
CoS queues : 8 supported
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : None
SONET defects : None
SONET errors:
Received path trace: routerb so-1/1/2
Transmitted path trace: routera so-4/1/2
show interfaces policers (SRX devices)

user@host> show interfaces policers

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Proto</th>
<th>Input Policer</th>
<th>Output Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>iso</td>
</tr>
<tr>
<td>gr-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mt-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pd-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pe-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>so-2/0/0.0-in-policer so-2/0/0.0-out-policer</td>
</tr>
<tr>
<td>iso</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show interfaces policers interface-name (SRX devices)

user@host> show interfaces policers so-2/1/0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Proto</th>
<th>Input Policer</th>
<th>Output Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-2/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/1/0.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>so-2/1/0.0-in-policer so-2/1/0.0-out-policer</td>
</tr>
<tr>
<td>iso</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inet6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show interfaces queue (SRX devices)

The following truncated example shows the CoS queue sizes for queues 0, 1, and 3. Queue 1 has a queue buffer size (guaranteed allocated memory) of 9192 bytes.

user@host> show interfaces queue

Physical interface: ge-0/0/0, Enabled, Physical link is Up
Interface index: 134, SNMP ifIndex: 509
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: class0
Queued:
- Packets : 0 0 pps
- Bytes   : 0 0 bps
Transmitted:
- Packets : 0 0 pps
- Bytes   : 0 0 bps
- Tail-dropped packets : 0 0 pps
- RL-dropped packets   : 0 0 pps
- RL-dropped bytes    : 0 0 bps
- RED-dropped packets : 0 0 pps
- Low                : 0 0 pps
- Medium-low          : 0 0 pps
- Medium-high         : 0 0 pps
- High               : 0 0 pps
- RED-dropped bytes  : 0 0 pps
- Low                : 0 0 bps

Copyright © 2019, Juniper Networks, Inc.
Interfaces Fundamentals for Routing Devices

show interfaces redundancy (SRX devices)

user@host> show interfaces redundancy

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Primary</th>
<th>Secondary</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsp0</td>
<td>Not present</td>
<td></td>
<td>sp-1/0/0</td>
<td>sp-0/2/0</td>
<td>both down</td>
</tr>
<tr>
<td>rsp1</td>
<td>On secondary</td>
<td>1d 23:56</td>
<td>sp-1/2/0</td>
<td>sp-0/3/0</td>
<td>primary down</td>
</tr>
<tr>
<td>rsp2</td>
<td>On primary</td>
<td>10:10:27</td>
<td>sp-1/3/0</td>
<td>sp-0/2/0</td>
<td>secondary down</td>
</tr>
<tr>
<td>rlsq0</td>
<td>On primary</td>
<td>00:06:24</td>
<td>lsq-0/3/0</td>
<td>lsq-1/0/0</td>
<td>both up</td>
</tr>
</tbody>
</table>

show interfaces redundancy (Aggregated Ethernet SRX devices)

user@host> show interfaces redundancy

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Primary</th>
<th>Secondary</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlsq0</td>
<td>On secondary</td>
<td>00:56:12</td>
<td>lsq-4/0/0</td>
<td>lsq-3/0/0</td>
<td>both up</td>
</tr>
<tr>
<td>ae0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show interfaces redundancy detail (SRX devices)

user@host> show interfaces redundancy detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlsq0</td>
<td>On primary</td>
<td>00:45:47</td>
</tr>
</tbody>
</table>
show interfaces routing brief (SRX devices)

```
show interfaces routing brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-5/0/3.0</td>
<td>Down</td>
<td>ISO enabled</td>
</tr>
<tr>
<td>so-5/0/2.0</td>
<td>Up</td>
<td>MPLS enabled, ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.2.120</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>so-5/0/1.0</td>
<td>Up</td>
<td>MPLS enabled, ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.2.130</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>at-1/0/0.3</td>
<td>Up</td>
<td>CCC enabled</td>
</tr>
<tr>
<td>at-1/0/0.2</td>
<td>Up</td>
<td>CCC enabled</td>
</tr>
<tr>
<td>at-1/0/0.0</td>
<td>Up</td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.90.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>lo0.0</td>
<td>Up</td>
<td>ISO 47.0005.80ff.f800.0000.0108.0001.1921.6800.5061.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 127.0.0.1</td>
</tr>
<tr>
<td>fxp1.0</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>fxp0.0</td>
<td>Up</td>
<td>INET 192.168.6.90</td>
</tr>
</tbody>
</table>
```

show interfaces routing detail (SRX devices)

```
show interfaces routing detail

so-5/0/3.0
Index: 15, Refcount: 2, State: Up <Broadcast PointToPoint Multicast> Change:<> Metric: 0, Up/down transitions: 0, Full-duplex
Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps ISO address (null)
State: <Broadcast PointToPoint Multicast> Change: <> Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes

so-5/0/2.0
Index: 14, Refcount: 7, State: <Up Broadcast PointToPoint Multicast> Change:<> Metric: 0, Up/down transitions: 0, Full-duplex
Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps MPLS address (null)
State: <Up Broadcast PointToPoint Multicast> Change: <> Preference: 0 (120 down), Metric: 0, MTU: 4458 bytes ISO address (null)
```
show interfaces routing-instance all (SRX devices)

user@host> show interfaces terse routing-instance all

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-0/0/1</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1/24</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>192.168.4.28/24</td>
<td>sample-a</td>
</tr>
<tr>
<td>at-0/1/0.0</td>
<td>up</td>
<td>up</td>
<td>inet6</td>
<td>fe80::a0:0:4/64</td>
<td>sample-b</td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1/32</td>
<td></td>
</tr>
</tbody>
</table>

show interfaces snmp-index (SRX devices)

user@host> show interfaces snmp-index 33

Physical interface: so-2/1/1, Enabled, Physical link is Down
Interface index: 149, SNMP ifIndex: 33
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
CoS queues : 8 supported
Input rate: 0 bps (0 pps)
Output rate: 0 bps (0 pps)
SONET alarms: LOL, PLL, LOS
SONET defects: LOL, PLL, LOF, LOS, SEF, AIS-L, AIS-P

show interfaces source-class all (SRX devices)

user@host> show interfaces source-class all

Logical interface so-0/1/0.0

<table>
<thead>
<tr>
<th>Source class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>1928095</td>
<td>161959980 597762</td>
</tr>
<tr>
<td>bronze</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface so-0/1/3.0

<table>
<thead>
<tr>
<th>Source class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bronze</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces statistics (Fast Ethernet SRX devices)

```
user@host> show interfaces fe-1/3/1 statistics

Physical interface: fe-1/3/1, Enabled, Physical link is Up
Interface index: 144, SNMP ifIndex: 1042
Description: ford fe-1/3/1
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues : 4 supported, 4 maximum usable queues
Current address: 00:90:69:93:04:dc, Hardware address: 00:90:69:93:04:dc
Last flapped : 2006-04-18 03:08:59 PDT (00:01:24 ago)
Statistics last cleared: Never
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
Input errors: 0, Output errors: 0
Active alarms : None
Active defects : None
Logical interface fe-1/3/1.0 (Index 69) (SNMP ifIndex 50)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500
Flags: Is-Primary, DCU, SCU-in

<table>
<thead>
<tr>
<th>Destination class</th>
<th>(packet-per-second)</th>
<th>(bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>silver1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0)</td>
<td>(0)</td>
<td></td>
</tr>
<tr>
<td>silver2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0)</td>
<td>(0)</td>
<td></td>
</tr>
<tr>
<td>silver3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0)</td>
<td>(0)</td>
<td></td>
</tr>
</tbody>
</table>

Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 10.27.245/24, Local: 10.27.245.2, Broadcast: 10.27.245.255
Protocol iso, MTU: 1497
Flags: Is-Primary
```

show interfaces switch-port (SRX devices)

```
user@host# show interfaces ge-slot/0/0 switch-port port-number

Port 0, Physical link is Up
Speed: 100mbps, Auto-negotiation: Enabled
Statistics:  
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total bytes</td>
<td>28437086</td>
<td>21792250</td>
</tr>
<tr>
<td>Total packets</td>
<td>409145</td>
<td>88008</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>9987</td>
<td>83817</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>145002</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>254156</td>
<td>4191</td>
</tr>
<tr>
<td>Multiple collisions</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td>FIFO/CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Runt frames</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Copyright © 2019, Juniper Networks, Inc.
show interfaces transport pm (SRX devices)

```
user@host> show interfaces transport pm all current et-0/1/0

Physical interface: et-0/1/0, SNMP ifIndex 515

<table>
<thead>
<tr>
<th>Near End</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
<th>COUNT</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU-BBE</td>
<td>0</td>
<td>800</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-ES</td>
<td>0</td>
<td>135</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-SES</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-UAS</td>
<td>427</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Far End</th>
<th>Suspect Flag:True</th>
<th>Reason:Unknown</th>
<th>COUNT</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU-BBE</td>
<td>0</td>
<td>800</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-ES</td>
<td>0</td>
<td>135</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-SES</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OTU-UAS</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Near End</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
<th>COUNT</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODU-BBE</td>
<td>0</td>
<td>800</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-ES</td>
<td>0</td>
<td>135</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-SES</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-UAS</td>
<td>427</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Far End</th>
<th>Suspect Flag:True</th>
<th>Reason:Unknown</th>
<th>COUNT</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODU-BBE</td>
<td>0</td>
<td>800</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-ES</td>
<td>0</td>
<td>135</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-SES</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODU-UAS</td>
<td>0</td>
<td>90</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FEC PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
<th>COUNT</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEC-CorrectedErr</td>
<td>2008544300</td>
<td>0</td>
<td>NA</td>
<td>NA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FEC-UncorrectedWords</td>
<td>0</td>
<td>0</td>
<td>NA</td>
<td>NA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BER PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
<th>MIN</th>
<th>MAX</th>
<th>AVG</th>
<th>THRESHOLD</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>BER</td>
<td>3.6e-5</td>
<td>5.8e-5</td>
<td>3.6e-5</td>
<td>10.0e-3</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Yes

Physical interface: et-0/1/0, SNMP ifIndex 515

<table>
<thead>
<tr>
<th>Suspect Flag:True</th>
<th>Reason:Object Disabled</th>
<th>TCA-ENABLED</th>
<th>TCA-RAISED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CURRENT</td>
<td>MIN</td>
<td>MAX</td>
<td>AVG</td>
</tr>
</tbody>
</table>

---
### Lane Chromatic Dispersion

- Lane chromatic dispersion: 0 NA NA NA NA
- Lane differential group delay: 0 NA NA NA NA

### q Value

- q Value: 120 120 120 120 0

### SNR

- SNR: 28 28 29 28 0

### Tx Output Power (0.01dBm)

- Tx output power: -5000 -5000 -5000 -5000 -300

### Rx Input Power (0.01dBm)

- Rx input power: -3642 -3665 -3626 -3637 -1800

### Module Temperature (Celsius)

- Module temperature: 46 46 46 46 46

### Tx Laser Bias Current (0.1mA)

- Tx laser bias current: 0 0 0 0 0

### Rx Laser Bias Current (0.1mA)

- Rx laser bias current: 1270 1270 1270 1270 0

### Carrier Frequency Offset (MHz)

- Carrier frequency offset: -186 -186 -186 -186 -5000

---

**show security zones (SRX devices)**

```
user@host> show security zones

Functional zone: management
   Description: This is the management zone.
   Policy configurable: No
   Interfaces bound: 1
   Interfaces:
      ge-0/0/0.0

Security zone: Host
   Description: This is the host zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
      fxp0.0

Security zone: abc
   Description: This is the abc zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
      ge-0/0/1.0

Security zone: def
   Description: This is the def zone.
   Send reset for non-SYN session TCP packets: Off
   Policy configurable: Yes
   Interfaces bound: 1
   Interfaces:
      ge-0/0/2.0
```
**show interfaces (ATM)**

**Syntax**

```
show interfaces atm/fpc/pic/port
<br|de|ext|te>
<des>
<me>
<snmp-index snmp-index>
<st>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

(M Series and T Series routers only) Display status information about the specified ATM interface.

**Options**

- `at-fpc/pic/port`—Display standard information about the specified ATM interface.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `snmp-index snmp-index`—(Optional) Display the SNMP index of the interface.

**Required Privilege Level**

`view`

**List of Sample Output**

- show interfaces (ATM, IMA Group) on page 1259
- show interfaces extensive (ATM IMA Group) on page 1260
- show interfaces (ATM1, SONET Mode) on page 1261
- show interfaces brief (ATM1, SONET Mode) on page 1262
- show interfaces detail (ATM1, SONET Mode) on page 1262
- show interfaces extensive (ATM1, SONET Mode) on page 1263
- show interfaces (ATM2, SDH Mode) on page 1266
- show interfaces brief (ATM2, SDH Mode) on page 1266
- show interfaces detail (ATM2, SDH Mode) on page 1267
- show interfaces extensive (ATM2, SDH Mode) on page 1269
- show interfaces (ATM2, SONET Mode) on page 1271
- show interfaces brief (ATM2, SONET Mode) on page 1273
- show interfaces detail (ATM2, SONET Mode) on page 1273
- show interfaces extensive (ATM2, SONET Mode) on page 1276

**Output Fields**

Table 33 on page 1245 lists the output fields for the `show interfaces` (ATM) command. Output fields are listed in the approximate order in which they appear.
### Table 33: ATM show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical interface</strong></td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Description</td>
<td>Configured interface description.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>details extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>details extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>details extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• ATM-CCC-CELL-RELAY—ATM cell relay for CCC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-CCC-VC-MUX—ATM virtual circuit (VC) for CCC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-CISCO-NLPID—Cisco-compatible ATM NLPID encapsulation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-MIPP-LLC—ATM MLPPP over ATM Adaptation Layer 5 (AAL5)/logical link control (LLC).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-NLPID—ATM NLPID encapsulation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-PPP-LLC—ATM PPP over AAL5/LLC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-PPP-VC-MUX—ATM PPP over raw AAL5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-PVC—ATM permanent virtual circuits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-SNAP—ATM LLC/SNAP encapsulation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-TCC-SNAP—ATM LLC/SNAP for translational cross-connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-TCC-VC-MUX—ATM VC for translational cross-connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ATM-VC-MUX—ATM VC multiplexing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ETHER-OVER-ATM-LLC—Ethernet over ATM (LLC/SNAP) encapsulation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ETHER-VPLS-OVER-ATM-LLC—Ethernet VPLS over ATM (bridging) encapsulation.</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>framing Mode</td>
<td>Framing mode: SONET or SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running as represented by the interface type (for example, OC3, ADSL2+, and SHDSL(2-wire)).</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>Payload scrambler</td>
<td>Whether payload scrambling is enabled.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 33: ATM show 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><strong>Device flags</strong></td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Link flags</strong></td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Hold-times</strong></td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Current address</strong></td>
<td>Ethernet MAC address for this interface for Ethernet over ATM encapsulation.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Input Rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Output Rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Statistics for traffic on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 33: ATM show 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><strong>Input errors</strong></td>
<td>Input errors on the interface whose definitions are as follows:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and frame check sequence (FCS)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s random early detection (RED) mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid VCs</strong>—Number of cells that arrived for a nonexistent VC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Sum of AAL5 packets that have FCS errors, reassembly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>timeout errors, and length errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discarded because they were not recognized or not of interest. Usually, this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

| **Output errors** | Output errors on the interface. The following paragraphs explain the counters     | extensive       |
|                   | whose meaning might not be obvious:                                               |                 |
|                   | • **Carrier transitions**—Number of times the interface has gone from down to up. |                 |
|                   |   This number does not normally increment quickly, increasing only when the       |                 |
|                   |   cable is unplugged, the far-end system is powered down and up, or another       |                 |
|                   |   problem occurs. If the number of carrier transitions increments quickly,        |                 |
|                   |   increasing only when the cable is unplugged, the far-end system is powered     |                 |
|                   |   down and then up, or another problem occurs. If it increments quickly (perhaps   |                 |
|                   |   once every 10 seconds), the cable, the far-end system, or the PIC or PIM is     |                 |
|                   |   malfunctioning.                                                                  |                 |
|                   | • **Errors**—Sum of the outgoing frame aborts and FCS errors.                     |                 |
|                   | • **Drops**—Number of packets dropped by the output queue of the I/O Manager      |                 |
|                   |   ASIC. If the interface is saturated, this number increments once for every      |                 |
|                   |   packet that is dropped by the ASIC’s RED mechanism.                             |                 |
|                   | • **Aged packets**—Number of packets that remained so long in shared packet      |                 |
|                   |   SDRAM that the system automatically purged them. The value in this field        |                 |
|                   |   should never increment. If it does, it is most likely a software bug or possibly|                 |
|                   |   malfunctioning hardware.                                                        |                 |
|                   | • **MTU errors**—Number of packets larger than the MTU threshold.                 |                 |
|                   | • **Resource errors**—Sum of transmit drops.                                       |                 |

| **Egress queues** | Total number of egress queues supported on the specified interface.               | detail extensive |
### Table 33: ATM show 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><strong>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>SONET alarms</strong></td>
<td>SONET media-specific defects that prevent the interface from passing packets.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>SONET defects</strong></td>
<td>When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SONET PHY, SONET section, SONET line, and SONET path.</td>
<td>none</td>
</tr>
<tr>
<td><strong>SONET PHY</strong></td>
<td>Counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>State—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PLL Lock—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PHY Light—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td><strong>SONET section</strong></td>
<td>Counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>State—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BIP-B1—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEF—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOL—Loss of light</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOF—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ES-S—Errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SES-S—Severely errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEFS-S—Severely errored framing seconds (section)</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: ATM show 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><strong>SONET line</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B2</strong>—Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-L</strong>—Remote error indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-L</strong>—Remote defect indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-L</strong>—Alarm indication signal (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SF</strong>—Bit error rate fault signal failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SD</strong>—Bit error rate defect signal degradation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-L</strong>—Errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-L</strong>—Severely errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-L</strong>—Unavailable seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-LFE</strong>—Errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-LFE</strong>—Severely errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-LFE</strong>—Unavailable seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td><strong>SONET path</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B3</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-P</strong>—Remote error indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOP-P</strong>—Loss of pointer (path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-P</strong>—Path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-P</strong>—Path remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UNEQ-P</strong>—Path unequipped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLM-P</strong>—Path payload (signal) label mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-P</strong>—Errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-P</strong>—Severely errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-P</strong>—Unavailable seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-PFE</strong>—Errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-PFE</strong>—Severely errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-PFE</strong>—Unavailable seconds (far-end STS path)</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: ATM show 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>Received SONET overhead</td>
<td>Values of the received and transmitted SONET overhead:</td>
<td>extensive</td>
</tr>
<tr>
<td>Transmitted SONET overhead</td>
<td>• C2—Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• F1—Section user channel byte. This byte is set aside for the purposes of users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• K1 and K2—These bytes are allocated for APS signaling for the protection of the multiplex section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• J0—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal. Used to transmit a 1-byte fixed-length string or a 16-byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S1—Synchronization status. The S1 byte is located in the first STS-1 of an STS-N.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Z3 and Z4—Allocated for future use.</td>
<td></td>
</tr>
<tr>
<td>SDH alarms</td>
<td>SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SDH PHY, SDH regenerator section, SDH multiplex section, and SDH path.</td>
<td>All levels</td>
</tr>
<tr>
<td>SDH defects</td>
<td>SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SDH PHY, SDH regenerator section, SDH multiplex section, and SDH path.</td>
<td>All levels</td>
</tr>
<tr>
<td>SDH PHY</td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PLL Lock—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PHY Light—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td>SDH regenerator section</td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RS-BIP8—24-bit BIP for multiplex section overhead (B2 bytes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OOF—Out of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOS—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOF—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RS-ES—Errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RS-SES—Severely errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RS-SEFS—Severely errored framing seconds (regenerator section)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 33: ATM show 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><strong>SDH multiplex section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-BIP24</strong>—8-bit BIP for high-order path overhead (B3 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-FEBE</strong>—Far-end block error (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-FERF</strong>—Far-end remote fail (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-AIS</strong>—Alarm indication signal (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-ES</strong>—Errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-SES</strong>—Severely errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-UAS</strong>—Unavailable seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-ES-FE</strong>—Errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-SES-FE</strong>—Severely errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-UAS-FE</strong>—Unavailable seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td><strong>SDH path</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-BIP8</strong>—8-bit BIP for regenerator section overhead (B1 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FEBE</strong>—Far-end block error (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-LOP</strong>—Loss of pointer (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-AIS</strong>—High-order-path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FERF</strong>—Far-end remote fail (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UNEQ</strong>—Unequipped (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-PLM</strong>—Payload label mismatch (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES</strong>—Errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES</strong>—Severely errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS</strong>—Unavailable seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES-FE</strong>—Errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES-FE</strong>—Severely errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS-FE</strong>—Unavailable seconds (far-end high-order path)</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: ATM show 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>Received SDH overhead</td>
<td>Values of the received and transmitted SONET overhead:</td>
<td>extensive</td>
</tr>
<tr>
<td>Transmitted SDH overhead</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• C2—Signal label. This byte is allocated to identify the construction and content</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the STS-level SPE and for PDI-P.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• F1—Section user channel byte. This byte is set aside for the purposes of users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• K1 and K2—These bytes are allocated for APS signaling for the protection of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multiplex section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• J0—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This byte is used to transmit a 1-byte fixed-length string or a 16-byte message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>so that a receiving terminal in a section can verify its continued connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to the intended transmitter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S1—Synchronization status. The S1 byte is located in the first STS-1 of an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-N.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Z3 and Z4—These bytes are allocated for future use.</td>
<td></td>
</tr>
<tr>
<td>Received path trace</td>
<td>SONET/SDH interfaces allow path trace bytes to be sent inband across the</td>
<td>extensive</td>
</tr>
<tr>
<td>Transmitted path trace</td>
<td>SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>diagnose misconfigurations and network errors by setting the transmitted path</td>
<td></td>
</tr>
<tr>
<td></td>
<td>trace message so that it contains the system hostname and name of the physical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface. The received path trace value is the message received from the router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>at the other end of the fiber. The transmitted path trace value is the message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that this router transmits.</td>
<td></td>
</tr>
<tr>
<td>ATM Status</td>
<td>ATM state information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• HCS State—Status of the header check sequence. ATM uses the HCS field in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cell header in the cell delineation process to frame ATM cell boundaries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The HCS is an FCS-8 calculation over the first four octets of the ATM cell</td>
<td></td>
</tr>
<tr>
<td></td>
<td>header.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOC—Current loss of cell (LOC) delineation state. OK means that no LOC is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>currently asserted.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 33: ATM show 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>ATM Statistics</td>
<td>ATM statistics for the interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Uncorrectable HCS errors—Number of cells dropped because the cell delineation failed. These errors most likely indicate that a SONET/SDH layer problem has occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Correctable HCS errors—Number of correctable HCS errors that occurred. The cell delineation process can recover from these errors and locate the ATM cell boundary, although the framing process is not quite stable. The ATM cell is not dropped. This counter increases when the cell delineation process changes its state from present to sync (for example, when a cable is plugged into the interface).</td>
<td></td>
</tr>
</tbody>
</table>

The following error statistics are from the framer:

- **Tx cell FIFO overruns**—Number of overruns in the transmit FIFO.
- **Rx cell FIFO overruns**—Number of overruns in the receive FIFO.
- **Rx cell FIFO underruns**—Number of underruns in the receive FIFO.
- **Input cell count**—Number of ATM cells received by the interface (not including idle cells).
- **Output cell count**—Number of ATM cells transmitted by the interface (including idle cells).
- **Output idle cell count**—Number of idle cells sent by the port. When ATM has nothing to send, it sends idle cells to fill the timeslot.
- **Output VC queue drops**—Number of packets dropped by a port on the PIC. Packets are dropped because of queue limits on the VC.

The following error statistics are from the SAR:

- **Input no buffers**—Number of AAL5 packets dropped because no channel blocks or buffers were available to handle them.
- **Input length errors**—Number of AAL5 packets dropped because their length was incorrect. Usually, these errors occur because a cell has been corrupted or lost, or because the length field was corrupted. They can also mean the AAL5 length field was zero.
- **Input timeouts**—Number of AAL5 packets dropped because of a reassembly timeout.
- **Input invalid VCs**—Number of AAL5 packets dropped because the header was unrecognized (because the VC was not correct or not configured).
- **Input bad CRCs**—Number of AAL5 packets dropped because of frame check sequence errors.
- **Input OAM cell no buffers**—Number of received OAM cells or raw cells dropped because no buffers were available to handle them.
- **L2 circuit out-of-sequence packets**—(Layer 2 AAL5 mode) Number of AAL5 packets that are out of sequential order.
- **Denied packets count**—The number of packets dropped due to VLAN priority deny packets or due to an error forwarding configuration that might cause a negative frame length, that is, the stripping size is larger than the packet size.

<table>
<thead>
<tr>
<th>Packet Forwarding Engine configuration</th>
<th>Information about the configuration of the Packet Forwarding Engine:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Destination slot—FPC slot number.</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: ATM show 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>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>CoS transmit queue</strong>—Queue number and its associated user-configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td>forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth %</strong>—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth bps</strong>—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer %</strong>—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer usec</strong>—Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Priority</strong>—Queue priority: <strong>low</strong> or <strong>high</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Limit</strong>—Displayed if rate limiting is configured for the queue. Possible</td>
<td></td>
</tr>
<tr>
<td></td>
<td>values are <strong>none</strong> and <strong>exact</strong>. If <strong>exact</strong> is configured, the queue</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmits only up to the configured bandwidth, even if excess bandwidth is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>available. If <strong>none</strong> is configured, the queue transmits beyond the configured</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 33: ATM show 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>VPI</td>
<td>(ATM2) Virtual path identifier information:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Flags—VPI flags can be one or more of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Active (virtual path is up)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OAM (operation and maintenance is enabled)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shaping (shaping is configured)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CBR, Peak</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OAM, Period—Interval at which OAM F4 loopback cells are sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Up count—Number of F4 OAM cells required to consider the virtual path up; the range is 1 through 255.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down count—Number of F4 OAM cells required to consider the virtual path down; the range is 1 through 255.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total down time—Total number of seconds the VPI has been down since it was opened, using the format Total down time: hh:mm:ss or Never.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last down—Time of last Down transition, using the format Last down: hh:mm:ss ago or Never.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OAM F4 cell statistics—(Nonpromiscuous mode) OAM F4 statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total received—Number of OAM F4 cells received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total sent—Number of OAM F4 cells sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loopback received—Number of OAM F4 loopback cells received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loopback sent—Number of OAM F4 loopback cells sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last received—Time at which the last OAM F4 cell was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last sent—Time at which the last OAM F4 cell was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RDI received—Number of OAM F4 cells received with the remote defect indication bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RDI sent—Number of OAM F4 cells sent with the RDI bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS received—Number of OAM F4 cells received with the alarm indication signal bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS sent—Number of OAM F4 cells sent with the AIS bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the VPI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the VPI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the VPI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the VPI.</td>
<td></td>
</tr>
</tbody>
</table>

### Logical Interface

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</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>Flags</td>
<td>Information about the logical interface. Possible values are described in the</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>&quot;Logical Interface Flags&quot; section under &quot;Common Output Fields Description&quot; on page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1152.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the logical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface. These statistics are the sum of the local and transit statistics.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When a burst of traffic is received, the value in the output packet rate field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>might briefly exceed the peak cell rate. It takes a while (generally, less than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 second) for this counter to stabilize.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>When a burst of traffic is received, the value in the output packet rate field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>might briefly exceed the peak cell rate. It takes a while (generally, less than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 second) for this counter to stabilize.</td>
<td></td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router. When a burst of traffic is</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>received, the value in the output packet rate field might briefly exceed the peak</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cell rate. It takes a while (generally, less than 1 second) for this counter to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>stabilize.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td>IP address of the interface is also displayed.</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>refers to the routing table inet.0.</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>the &quot;Family Flags&quot; section under &quot;Common Output Fields Description&quot; on page</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>1152.</td>
<td></td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>&quot;Addresses Flags&quot; section under &quot;Common Output Fields Description&quot; on page</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>1152.</td>
<td></td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
### Table 33: ATM show 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>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>VCI</td>
<td>Virtual circuit identifier number and information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td><strong>Flags</strong>—VCI flags:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—VCI is up and in working condition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CCC down</strong>—VCI CCC is not in working condition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—VCI is closed because the user disabled the logical or physical interface from the CLI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Configured</strong>—VCI is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—VCI is not in working condition. The VCI might have alarms, defects, F5 AIS/RDI, or no response to OAM loopback cells.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ILMI</strong>—VCI is up and in working condition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>OAM</strong>—OAM loopback is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Multicast</strong>—VCI is a multicast VCI or DLCI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Multipoint destination</strong>—VCI is configured as a multipoint destination.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No VCI flags.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Passive-OAM</strong>—Passive OAM is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Shaping</strong>—Shaping is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Sustained</strong>—Shaping rate is set to <strong>Sustained</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unconfigured</strong>—VCI is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Total down time</strong>—Total number of seconds the VCI has been down, using the format <strong>Total down time: hh:mm:ss or Never.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Last down</strong>—Time of last <strong>Down</strong> transition, using the format <strong>Last down: hh:mm:ss.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>EPD threshold</strong>—(ATM2 only) Threshold at which a packet is dropped when the queue size (in number of cells) exceeds the early packet-discard (EPD) value.</td>
<td></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>VCI (continued)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmit weight cells—(ATM2 only) Amount of bandwidth assigned to this queue.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• ATM per-VC transmit statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tail queue packet drops—Number of packets dropped because of bandwidth constraints. This value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates that packets are queued to send out at a rate faster than allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OAM F4 cell statistics—(Nonpromiscuous mode) OAM F4 statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total received—Number of OAM F4 cells received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total sent—Number of OAM F4 cells sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loopback received—Number of OAM F4 loopback cells received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loopback sent—Number of OAM F4 loopback cells sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last received—Time at which the last OAM F4 cell was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last sent—Time at which the last OAM F4 cell was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RDI received—Number of OAM F4 cells received with the remote defect indication bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RDI sent—Number of OAM F4 cells sent with the RDI bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS received—Number of OAM F4 cells received with the alarm indication signal bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS sent—Number of OAM F4 cells sent with the AIS bit set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Traffic statistics—Number and rate of bytes and packets received and transmitted on the physical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMA group properties</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Version—The specified IMA specification version, either IMA 1.0 or IMA 1.1.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Frame length—The specified frame size, which can be 32, 64, 128, or 256.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Differential delay—Maximum differential delay among links in milliseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Symmetry—Either Common Transmit Clock or Independent Transmit Clock timing mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmit clock—The specified IMA clock mode, either common or independent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Minimum links—The number of minimum active links specified in both transmit and receive directions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmit—The per-PIC limit on the number of minimum active links in the transmit direction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Receive—The per-PIC limit on the number of minimum active links in the receive direction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Frame synchronization—The specified IMA frame synchronization state transition variables (Alpha, Beta, and Gamma) and their specified values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Alpha—The number of consecutive invalid ICP cells for IFSM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Beta—The number of consecutive errored ICP cells for IFSM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Gamma—The number of consecutive valid ICP cells for IFSM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Links—The number of IMA links assigned to the IMA group.</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: ATM show 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>IMA group alarms</td>
<td>• Start-up-FE—Far-end group alarm status</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Config-Aborted—Near-end configuration aborted group alarm status</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Config-Aborted-FE—Far-end configuration aborted group alarm status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Insufficient-Links—Near-end insufficient links group alarm status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Insufficient-Links-FE—Far-end insufficient links group alarm status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Blocked-FE—Far-end blocked group alarm status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GR-Timing-Mismatch—Group timing mismatch alarm status</td>
<td></td>
</tr>
<tr>
<td>IMA group defects</td>
<td>• Start-up-FE—Far-end group defect status</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Config-Aborted—Near-end configuration aborted group defect status</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Config-Aborted-FE—Far-end configuration aborted group defect status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Insufficient-Links—Near-end insufficient links group defect status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Insufficient-Links-FE—Far-end insufficient links group defect status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Blocked-FE—Far-end blocked group defect status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GR-Timing-Mismatch—Group timing mismatch defect status</td>
<td></td>
</tr>
<tr>
<td>IMA Group state</td>
<td>Near-end and far-end group status</td>
<td>detail extensive</td>
</tr>
<tr>
<td>IMA group media</td>
<td>IMA group media status, including seconds, count and state for the following</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>media parameters:</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• FC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FC-FE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Addr-Mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Running</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UAS</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show interfaces (ATM, IMA Group)

```
user@host> show interfaces at-1/0/0
Physical interface: at-1/0/0, Enabled, Physical link is Up
IMA group properties:
  Version : 1.1
  Frame length : 128
  Differential delay : 25 milliseconds
  Symmetry : Symmetrical Configuration and Operation
  Transmit clock : Common
  Minimum links : Transmit: 1, Receive: 1
  Frame synchronization: Alpha: 2, Beta: 2, Gamma: 1
  Links : None
IMA group alarms : Start-up-FE Config-Aborted Config-Aborted-FE
  Insufficient-Links Insufficient-Links-FE Blocked-FE GR-Timing-Mismatch
IMA group defects : Start-up-FE Config-Aborted Config-Aborted-FE
  Insufficient-Links Insufficient-Links-FE Blocked-FE GR-Timing-Mismatch
IMA Group state:
  Near end : Start up
```
show interfaces extensive (ATM IMA Group)

user@host> show interfaces at-0/0/10 extensive

Physical interface: at-0/0/10, Enabled, Physical link is Up
  Interface index: 178, SNMP ifIndex: 540, Generation: 531
  Link-level type: ATM-PVC, MTU: 2048, Speed: Unspecified, Loopback: None, Payload
  scrambler: Enabled
  Device flags : Present Running
  Link flags : None
  CoS queues : 8 supported, 4 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:0a
  Last flapped : 2012-03-16 16:49:15 PDT (2d 07:12 ago)
  Statistics last cleared: 2012-03-16 16:56:58 PDT (2d 07:05 ago)

Traffic statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets : 0 0 pps
  Output packets : 0 0 pps

IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets : 0
  Output packets : 0

Input errors:
  Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, Resource errors: 0

Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0, Resource errors: 0

IMA group properties:
  Version : 1.1
  Frame length : 128
  Differential delay : 25 milliseconds
  Symmetry : Symmetrical Configuration and Operation
  Transmit clock : Common
  Minimum links : Transmit: 1, Receive: 1
  Frame synchronization: Alpha: 2, Beta: 2, Gamma: 1
  Link #1 : t1-0/0/4 up

IMA Group alarms : None
IMA Group defects : None

IMA Group state:
  Near end : Operational
  Far end : Operational

IMA group media: Seconds Count State
  FC  0
  FC-FE  0
  Addr-Mismatch  0
  Running 198306
show interfaces (ATMI, SONET Mode)

user@host> show interfaces at-0/0/0

Physical interface: at-0/0/0, Enabled, Physical link is Up
  Interface index: 300, SNMP ifIndex: 194
  Description: to allspice at-0/0/0
  Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
  Speed: OC3, Loopback: None, Payload scrambler: Enabled
  Device flags    : Present Running
  Link flags      : None
  CoS queues      : 4 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:fe
  Last flapped    : 2006-02-24 14:28:12 PST (6d 01:51 ago)
  Input rate      : 0 bps (0 pps)
  Output rate     : 0 bps (0 pps)
  SONET alarms    : None
  SONET defects   : None

Logical interface at-0/0/0.0 (Index 64) (SNMP ifIndex 204)
  Flags: Point-To-Point SNMP-Traps Encapsulation: ATM-SNAP
  Input packets   : 0
  Output packets  : 0
  Protocol inet, MTU: 4470
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 192.168.220.24/30, Local: 192.168.220.26,
      Broadcast: 192.168.220.27
  Protocol iso, MTU: 4470
    Flags: None
show interfaces brief (ATM1, SONET Mode)

```
show interfaces at-1/0/0 brief

Physical interface: at-1/0/0, Enabled, Physical link is Up
Description: to allspice at-1/0/0
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
Speed: OC3, Loopback: None, Payload scrambler: Enabled
Device flags   : Present Running
Link flags     : None

Logical interface at-1/0/0.0
Flags: Point-To-Point SNMP-Traps Encapsulation: ATM-SNAP
inet  192.168.220.26/30
iso
VCI 0.128
Flags: Active
Total down time: 0 sec, Last down: Never
```

show interfaces detail (ATM1, SONET Mode)

```
show interfaces at-1/0/0 detail

Physical interface: at-1/0/0, Enabled, Physical link is Up
Interface index: 300, SNMP ifIndex: 194, Generation: 183
Description: to allspice at-1/0/0
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
Speed: OC3, Loopback: None, Payload scrambler: Enabled
Device flags   : Present Running
Link flags     : None
CoS queues     : 4 supported, 4 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:fe
Last flapped   : 2006-02-24 14:28:12 PST (6d 01:55 ago)
Statistics last cleared: Never
Traffic statistics:
Input  bytes  :                    0                    0 bps
Output bytes  :                    0                    0 bps
Input  packets:                    0                    0 pps
Output packets:                    0                    0 pps
Egress queues: 4 supported, 4 in use
Queue counters:       Queued packets      Transmitted packets      Dropped packets
0 best-effort                    0                    0                    0
1 expedited-fo                 0                    0                    0
2 assured-forw                0                    0                    0
3 network-cont                 0                    0                    0
SONET alarms     : None
SONET defects    : None
```
Logical interface at-1/0/0.0 (Index 64) (SNMP ifIndex 204) (Generation 5)
Flags: Point-To-Point SNMP-Traps Encapsulation: ATM-SNAP
Traffic statistics:
- Input bytes : 0
- Output bytes : 0
- Input packets: 0
- Output packets: 0
Local statistics:
- Input bytes : 0
- Output bytes : 0
- Input packets: 0
- Output packets: 0
Transit statistics:
- Input bytes : 0 0 bps
- Output bytes : 0 0 bps
- Input packets: 0 0 pps
- Output packets: 0 0 pps
Protocol inet, MTU: 4470, Generation: 13, Route table: 0
  Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 192.168.220.24/30, Local: 192.168.220.26,
  Broadcast: 192.168.220.27, Generation: 14
Protocol iso, MTU: 4470, Generation: 14, Route table: 0
  Flags: None
VCI 0.128
  Flags: Active
  Total down time: 0 sec, Last down: Never
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
Traffic statistics:
- Input bytes : 0
- Output bytes : 0
- Input packets: 0
- Output packets: 0
Input errors:
  Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
Resource errors: 0
Egress queues: 4 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets
0 best-effort                    0                    0                    0
1 expedited-fo                   0                    0                    0
2 assured-forw                   0                    0                    0
3 network-cont                   0                    0                    0
SONET alarms   : None
SONET defects  : None
SONET PHY:
PLL Lock                  0            0  OK
PHY Light                 0            0  OK
SONET section:
  BIP-B1                    0            0
  SEF                       0            0  OK
  LOS                       0            0  OK
  LOF                       0            0  OK
  ES-S                      0
  SES-S                     0
  SEFS-S                    0
SONET line:
  BIP-B2                    0            0
  REI-L                     0            0
  RDI-L                     0            0  OK
  AIS-L                     0            0  OK
  BERR-SF                   0            0  OK
  BERR-SD                   0            0  OK
  ES-L                      0
  SES-L                     0
  UAS-L                     0
  ES-LFE                    0
  SES-LFE                   0
  UAS-LFE                   0
SONET path:
  BIP-B3                    0            0
  REI-P                     0            0
  LOP-P                     0            0  OK
  AIS-P                     0            0  OK
  RDI-P                     0            0  OK
  UNEQ-P                    1            1  OK
  PLM-P                     0            0  OK
  ES-P                      1
  SES-P                     1
  UAS-P                     0
  ES-PFE                    0
  SES-PFE                   0
  UAS-PFE                   0
Received SONET overhead:
  F1      : 0x00, J0      : 0x00, K1 : 0x00, K2 : 0x00
  S1      : 0x00, C2      : 0x13, C2(cmp) : 0x13, F2 : 0x00
Z3 : 0x00, Z4 : 0x00, S1(cmp) : 0x00
Transmitted SONET overhead:
F1 : 0x00, J0 : 0x01, K1 : 0x00, K2 : 0x00
S1 : 0x00, C2 : 0x13, F2 : 0x00, Z3 : 0x00
Z4 : 0x00
ATM status:
HCS state: Sync
LOC : OK
ATM Statistics:
Uncorrectable HCS errors: 0, Correctable HCS errors: 0,
Tx cell FIFO overruns: 0, Rx cell FIFO overruns: 0,
Rx cell FIFO underruns: 0, Input cell count: 0, Output cell count: 0,
Output idle cell count: 0, Output VC queue drops: 0, Input no buffers: 0,
Input length errors: 0, Input timeouts: 0, Input invalid VCs: 0,
Input bad CRCs: 0, Input OAM cell no buffers: 0
Packet Forwarding Engine configuration:
Destination slot: 1
CoS Information:
CoS transmit queue  Bandwidth  Buffer  Priority  Limit
%        bps    %     usec         %
0 best-effort  95  147744000  95  0    low    none
3 network-control  5  77760000    5  0    low    none
Logical interface at-1/0/0.0 (Index 64) (SNMP ifIndex 204) (Generation 5)
Flags: Point-To-Point SNMPP-Traps Encapsulation: ATM-SNAP
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: 4470, Generation: 13, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 192.168.220.24/30, Local: 192.168.220.26,
  Broadcast: 192.168.220.27, Generation: 14
Protocol iso, MTU: 4470, Generation: 14, Route table: 0
Flags: None
VCI 0.128
Flags: Active
Total down time: 0 sec, Last down: Never
ATM per-VC transmit statistics:
  Tail queue packet drops: 0
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
show interfaces (ATM2, SDH Mode)

user@host> show interfaces at-0/2/1

Physical interface: at-0/2/1, Enabled, Physical link is Up
Interface index: 154, SNMP ifIndex: 42
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SDH mode, Speed: OC3,
Loopback: None, Payload scrambler: Enabled
Device flags : Present Running
Link flags : None
CoS queues : 4 supported, 4 maximum usable queues
Current address: 00:00:5e:00:53:3f
Last flapped : 2006-03-24 13:29:58 PST (00:04:48 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SDH alarms : None
SDH defects : None
VPI 0 Flags: Active
Total down time: 0 sec, Last down: Never
Traffic statistics:
  Input packets: 0
  Output packets: 0

Logical interface at-0/2/1.0 (Index 75) (SNMP ifIndex 51)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: ATM-SNAP
Input packets : 0
Output packets: 0
Protocol inet, MTU: 4470
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.12.6, Local: 10.0.12.5
Protocol iso, MTU: 4470
  Flags: None
VCI 0.128
  Flags: Active
  Total down time: 0 sec, Last down: Never
  EPD threshold: 2129, Transmit weight cells: 0
    Input packets : 0
    Output packets: 0

Logical interface at-0/2/1.32767 (Index 76) (SNMP ifIndex 50)
Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x4000 Encapsulation: ATM-VCMUX
Input packets : 0
Output packets: 0
VCI 0.4
  Flags: Active
  Total down time: 0 sec, Last down: Never
  EPD threshold: 0, Transmit weight cells: 0
    Input packets : 0
    Output packets: 0

show interfaces brief (ATM2, SDH Mode)

user@host> show interfaces at-0/2/1 brief

Physical interface: at-0/2/1, Enabled, Physical link is Up
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SDH mode,
show interfaces detail (ATM2, SDH Mode)

user@host> show interfaces at-0/2/1 detail

Physical interface: at-0/2/1, Enabled, Physical link is Up
Interface index: 154, SNMP ifIndex: 42, Generation: 40
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SDH mode, Speed: OC3,

Loopback: None, Payload scrambler: Enabled
Device flags : Present Running
Link flags : None
CoS queues : 4 supported, 4 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:3f
Last flapped : 2006-03-24 13:29:58 PST (00:05:10 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Egress queues: 4 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 0 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 0 0 0
SDH alarms : None
SDH defects : None
VPI 0
Flags: Active
Total down time: 0 sec, Last down: Never
Traffic statistics:
Input bytes : 0
Output bytes : 0
Logical interface at-0/2/1.0 (Index 75) (SNMP ifIndex 51) (Generation 25)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: ATM-SNAP
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
Protocol inet, MTU: 4470, Generation: 62, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.0.12.6, Local: 10.0.12.5, Broadcast: Unspecified,
  Generation: 58
Protocol iso, MTU: 4470, Generation: 63, Route table: 0
  Flags: None
VCI 0.128
  Flags: Active
  Total down time: 0 sec, Last down: Never
  EPD threshold: 2129, Transmit weight cells: 0
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Logical interface at-0/2/1.32767 (Index 76) (SNMP ifIndex 50) (Generation 26)
Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x4000
Encapsulation: ATM-VCMUX
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
VCI 0.4
  Flags: Active
  Total down time: 0 sec, Last down: Never
  EPD threshold: 0, Transmit weight cells: 0
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
show interfaces extensive (ATM2, SDH Mode)

user@host> show interfaces at-0/2/1 extensive

Physical interface: at-0/2/1, Enabled, Physical link is Up
Interface index: 154, SNMP ifIndex: 42, Generation: 40
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SDH mode, Speed: OC3,
Loopback: None, Payload scrambler: Enabled
Device flags : Present Running
Link flags     : None
CoS queues     : 4 supported, 4 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:3f
Last flapped   : 2006-03-24 13:29:58 PST (00:06:49 ago)
Traffic statistics:
Input  bytes  :                    0                    0 bps
Output bytes  :                    0                    0 bps
Input  packets:                    0                    0 pps
Output packets:                    0                    0 pps
Input errors:
    Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
    L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
    Resource errors: 0
Output errors:
    Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
    Resource errors: 0
Egress queues: 4 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets
0 best-effort                    0                    0                    0
1 expedited-fo                   0                    0                    0
2 assured-forw                   0                    0                    0
3 network-cont                   0                    0                    0
SDH alarms   : None
SDH defects  : None
SDH PHY:
    PLL Lock   0            0 OK
    PHY Light  1            1 OK
SDH regenerator section:
    RS-BIP8        2        8828
    OOF           2          2 OK
    LOS           2          1 OK
    LOF           2          1 OK
    RS-ES         4
    RS-SES        3
    RS-SEFS       2
SDH multiplex section:
    MS-BIP24      2         771
    MS-FEBE       1       17476
Interfaces Fundamentals for Routing Devices

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Error</th>
<th>Status</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-FERF</td>
<td>2</td>
<td>1 OK</td>
<td>MS-AIS</td>
<td>2</td>
</tr>
<tr>
<td>BERR-SF</td>
<td>0</td>
<td>0 OK</td>
<td>BERR-SD</td>
<td>0</td>
</tr>
<tr>
<td>MS-ES</td>
<td>4</td>
<td></td>
<td>MS-SES</td>
<td>2</td>
</tr>
<tr>
<td>MS-UAS</td>
<td>0</td>
<td></td>
<td>MS-ES-FE</td>
<td>3</td>
</tr>
<tr>
<td>MS-SES-FE</td>
<td>2</td>
<td></td>
<td>MS-UAS-FE</td>
<td>0</td>
</tr>
<tr>
<td>SDH path:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-BIP8</td>
<td>1</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-FEBE</td>
<td>1</td>
<td>251</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-LOP</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-AIS</td>
<td>2</td>
<td>1 OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-FERF</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UNEQ</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-PLM</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-ES</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-SES</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UAS</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-ES-FE</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-SES-FE</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDH overhead:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F1 : 0x00, J0 : 0x00, K1 : 0x00, K2 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S1 : 0x00, C2 : 0x13, C2(cmp) : 0x13, F2 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z3 : 0x00, Z4 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmitted SDH overhead:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F1 : 0x00, J0 : 0x01, K1 : 0x00, K2 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S1 : 0x00, C2 : 0x13, F2 : 0x00, Z3 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z4 : 0x00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ATM status:
HCS state: Sync
LOC: OK
ATM Statistics:
Uncorrectable HCS errors: 0, Correctable HCS errors: 0,
Rx cell FIFO overruns: 0, Tx cell FIFO overruns: 0,
Output cell count: 0, Input cell count: 0,
Output idle cell count: 0, Input idle cell count: 0,
Output VC queue drops: 0, Input no buffers: 0,
Input length errors: 0, Input timeouts: 0,
Input invalid VCs: 0, Input bad CRCs: 0,
Input OAM cell no buffers: 0
Packet Forwarding Engine configuration:
Destination slot: 0
VPI 0
Flags: Active
Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Logical interface at-0/2/1.0 (Index 75) (SNMP ifIndex 51) (Generation 25)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: ATM-SNAP
Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
show interfaces (ATM2, SONET Mode)

user@host> show interfaces at-0/3/1

Physical interface: at-0/3/1, Enabled, Physical link is Up
  Interface index: 139, SNMP ifIndex: 67
  Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
<table>
<thead>
<tr>
<th>Interface</th>
<th>Flags</th>
<th>EPD threshold</th>
<th>Transmit weight cells</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPI 0</td>
<td>Active, OAM, Shaping</td>
<td>2129</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VPI 10</td>
<td>Active</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Logical interface at-0/3/1.0</td>
<td>Point-To-Point Copy-PLP-To-CLP</td>
<td>2129</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Logical interface at-0/3/1.32767</td>
<td>Point-To-Multipoint Copy-PLP-To-CLP</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>30</td>
</tr>
</tbody>
</table>

**SONET alarms**: None
**SONET defects**: None

**Current address**: 00:00:5e:00:53:5e
**Last flapped**: 2006-03-13 17:46:36 PST (16:01:12 ago)
**Input rate**: 0 bps (0 pps)
**Output rate**: 0 bps (0 pps)
**Logical interface at-0/3/1.32767** (Index 79) (SNMP ifIndex 76)
**Flags**: Point-To-Multipoint Copy-PLP-To-CLP No-Multicast SNMP-Traps 0x4000
**Encapsulation**: ATM-VCMUX
**Input packets**: 4
**Output packets**: 30
**VCI 0.16**
**Flags**: Active, ILMI
**Total down time**: 0 sec, Last down: Never
**EPD threshold**: 0, Transmit weight cells: 0
**Input packets**: 0
**Output packets**: 26
show interfaces brief (ATM2, SONET Mode)

```
user@host> show interfaces at-0/3/1 brief

Physical interface: at-0/3/1, Enabled, Physical link is Up
   Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
   Speed: OC3, Loopback: None, Payload scrambler: Enabled
   Device flags   : Present Running
   Link flags     : None

Logical interface at-0/3/1.0
   Flags: Point-To-Point Copy-PLP-To-CLP SNMP-Traps 0x4000
   Encapsulation: ATM-SNAP
   inet 10.0.59.6 -- 10.0.59.5
   iso
   VCI 0.128
   Flags: Active
   Total down time: 0 sec, Last down: Never
   EPD threshold: 2129, Transmit weight cells: 10

Logical interface at-0/3/1.32767
   Flags: Point-To-Multipoint Copy-PLP-To-CLP No-Multicast SNMP-Traps 0x4000
   Encapsulation: ATM-VCMUX
   VCI 0.16
   Flags: Active, ILMI
   Total down time: 0 sec, Last down: Never
   EPD threshold: 0, Transmit weight cells: 0
   VCI 0.4
   Flags: Active, OAM
   Total down time: 0 sec, Last down: Never
   EPD threshold: 2129, Transmit weight cells: 0
```

show interfaces detail (ATM2, SONET Mode)

```
user@host> show interfaces at-0/3/1 detail

Physical interface: at-0/3/1, Enabled, Physical link is Up
   Interface index: 139, SNMP ifIndex: 67, Generation: 22
   Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
   Speed: OC3, Loopback: None, Payload scrambler: Enabled
   Device flags   : Present Running
   Link flags     : None
   CoS queues     : 4 supported, 4 maximum usable queues
   Hold-times     : Up 0 ms, Down 0 ms
   Current address: 00:00:5e:00:53:5e
   Last flapped   : 2006-03-13 17:46:36 PST (16:02:39 ago)
   Statistics last cleared: Never
   Traffic statistics:

Labeled cell statistics:
   Total received: 0, Total sent: 0
   Loopback received: 0, Loopback sent: 0
   RDI received: 0, RDI sent: 0
   AIS received: 0, AIS sent: 0
```

Chapter 14: Interface Operational Commands
<table>
<thead>
<tr>
<th>Input bytes :</th>
<th>312</th>
<th>Output bytes :</th>
<th>2952</th>
<th>Input packets:</th>
<th>6</th>
<th>Output packets:</th>
<th>50</th>
</tr>
</thead>
</table>

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>44</td>
<td>44</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

SONET alarms: None
SONET defects: None

VPI 0
Flags: Active, OAM, Shaping
CBR, Peak: 50kbps
OAM, Period 30 sec, Up count: 10, Down count: 10
Total down time: 0 sec, Last down: Never
OAM F4 cell statistics:
Total received: 6, Total sent: 6
Loopback received: 6, Loopback sent: 6
Last received: 00:00:29, Last sent: 00:00:29
RDI received: 0, RDI sent: 0
AIS received: 0
Traffic statistics:
Input bytes : 312
Output bytes : 2952
Input packets: 6
Output packets: 50

VPI 10
Flags: Active
Total down time: 0 sec, Last down: Never
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Logical interface at-0/3/1.0 (Index 78) (SNMP ifIndex 77) (Generation 20)
Flags: Point-To-Point Copy-PLP-To-CLP SNMP-Traps 0x4000
Encapsulation: ATM-SNAP
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Protocol inet, MTU: 4470, Generation: 38, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.59.5, Local: 10.0.59.6, Broadcast: Unspecified,
    Generation: 44
Protocol iso, MTU: 4470, Generation: 39, Route table: 0
  Flags: None
VCI 0.128
  Flags: Active
  Total down time: 0 sec, Last down: Never
  EPD threshold: 2129, Transmit weight cells: 10
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0

Logical interface at-0/3/1.32767 (Index 79) (SNMP ifIndex 76) (Generation 21)
  Flags: Point-To-Multipoint Copy-PLP-To-CLP No-Multicast SNMP-Traps 0x4000
  Encapsulation: ATM-VCMUX
  Traffic statistics:
    Input bytes : 360
    Output bytes : 3302
    Input packets: 6
    Output packets: 50
  Local statistics:
    Input bytes : 360
    Output bytes : 3302
    Input packets: 6
    Output packets: 50

VCI 0.16
  Flags: Active, ILMI
  Total down time: 0 sec, Last down: Never
  EPD threshold: 0, Transmit weight cells: 0
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
  Traffic statistics:
    Input bytes : 0
    Output bytes : 2640
    Input packets: 0
    Output packets: 44

VCI 0.4
  Flags: Active, OAM
  OAM, Period 30 sec, Up count: 10, Down count: 10
  Total down time: 0 sec, Last down: Never
  EPD threshold: 2129, Transmit weight cells: 0
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
  Traffic statistics:
    Input bytes : 312
    Output bytes : 312
    Input packets: 6
    Output packets: 6
  OAM F4 cell statistics:
    Total received: 6, Total sent: 6
    Loopback received: 6, Loopback sent: 6
    Last received: 00:00:29, Last sent: 00:00:29
    RDI received: 0, RDI sent: 0
    AIS received: 0, AIS sent: 0
**show interfaces extensive (ATM2, SONET Mode)**

```
user@host> show interfaces at-0/3/1 extensive

Physical interface: at-0/3/1, Enabled, Physical link is Up
Interface index: 139, SNMP ifIndex: 67, Generation: 22
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, SONET mode,
Speed: OC3, Loopback: None, Payload scrambler: Enabled
Device flags : Present Running
Link flags : None
CoS queues : 4 supported, 4 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:5e
Last flapped : 2006-03-13 17:46:36 PST (16:04:12 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 520 0 bps
Output bytes : 4240 0 bps
Input packets: 10 0 pps
Output packets: 72 0 pps
Input errors:
Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
Resource errors: 0
Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
Resource errors: 0
Egress queues: 4 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort 62 62 0
  1 expedited-fo 0 0 0
  2 assured-forw 0 0 0
  3 network-cont 10 10 0
SONET alarms : None
SONET defects : None
SONET PHY:
PLL Lock 0 0 OK
PHY Light 0 0 OK
SONET section:
BIP-B1 0 0
SEF 0 0 OK
LOS 0 0 OK
LOF 0 0 OK
ES-S 0
SES-S 0
SEFS-S 0
SONET line:
BIP-B2 0 0
REI-L 0 0
RDI-L 0 0 OK
AIS-L 0 0 OK
BERR-SF 0 0 OK
BERR-SD 0 0 OK
```
ES-L                      0
SES-L                     0
UAS-L                     0
ES-LFE                    0
SES-LFE                   0
UAS-LFE                   0
SONET path:
BIP-B3                    0            0
REI-P                     0            0
LOP-P                     0            0  OK
AIS-P                     0            0  OK
RDI-P                     0            0  OK
UNEQ-P                    1            1  OK
PLM-P                     0            0  OK
ES-P                      1
SES-P                     1
UAS-P                     0
ES-PFE                    0
SES-PFE                   0
UAS-PFE                   0
Received SONET overhead:
F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0x13, C2(cmp) : 0x13, F2      : 0x00
Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00
Transmitted SONET overhead:
F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0x13, F2      : 0x00, Z3      : 0x00
Z4      : 0x00
ATM status:
HCS state:     Sync
LOC      :       OK
ATM Statistics:
Uncorrectable HCS errors: 0, Correctable HCS errors: 0,
Tx cell FIFO overruns: 0, Rx cell FIFO overruns: 0,
Rx cell FIFO underruns: 0, Input cell count: 0, Output cell count: 0,
Output idle cell count: 0, Output VC queue drops: 0, Input no buffers: 0,
Input length errors: 0, Input timeouts: 0, Input invalid VCs: 0,
Input bad CRCs: 0, Input OAM cell no buffers: 0
Packet Forwarding Engine configuration:
Destination slot: 0
VPI 0
Flags: Active, OAM, Shaping
CBR, Peak: 50kbps
OAM, Period 30 sec, Up count: 10, Down count: 10
Total down time: 0 sec, Last down: Never
OAM F4 cell statistics:
Total received: 10, Total sent: 10
Loopback received: 10, Loopback sent: 10
Last received: 00:00:02, Last sent: 00:00:02
RDI received: 0, RDI sent: 0
AIS received: 0
Traffic statistics:
  Input bytes :                       520
  Output bytes :                      4240
  Input packets:                       10
  Output packets:                      72
VPI 10
Flags: Active
Total down time: 0 sec, Last down: Never
Traffic statistics:
<table>
<thead>
<tr>
<th>Logical interface at-0/3/1.0 (Index 78) (SNMP ifIndex 77) (Generation 20)</th>
<th>Traffic statistics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: Point-To-Point Copy-PLP-To-CLP SNMP-Traps 0x4000</td>
<td>Input bytes : 0</td>
</tr>
<tr>
<td>Encapsulation: ATM-SNAP</td>
<td>Output bytes : 0</td>
</tr>
<tr>
<td>Traffic statistics:</td>
<td>Input packets: 0</td>
</tr>
<tr>
<td>Input bytes : 0</td>
<td>Output packets: 0</td>
</tr>
<tr>
<td>Output bytes : 0</td>
<td>Local statistics:</td>
</tr>
<tr>
<td>Input packets: 0</td>
<td>Output bytes : 0</td>
</tr>
<tr>
<td>Output packets: 0</td>
<td>Input packets: 0</td>
</tr>
<tr>
<td>Output packets: 0</td>
<td>Transit statistics:</td>
</tr>
<tr>
<td>Transit statistics:</td>
<td>Input bytes : 0</td>
</tr>
<tr>
<td>Input bytes : 0</td>
<td>Output bytes : 0</td>
</tr>
<tr>
<td>Output bytes : 0</td>
<td>Input packets: 0</td>
</tr>
<tr>
<td>Input packets: 0</td>
<td>Output packets: 0</td>
</tr>
<tr>
<td>Output packets: 0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol inet, MTU: 4470, Generation: 38, Route table: 0</th>
<th>Traffic statistics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: None</td>
<td>Input bytes : 660</td>
</tr>
<tr>
<td>Addresses, Flags: Is-Preferred Is-Primary</td>
<td>Output bytes : 5473</td>
</tr>
<tr>
<td>Destination: 10.0.59.5, Local: 10.0.59.6, Broadcast: Unspecified, Generation: 44</td>
<td>Input packets: 11</td>
</tr>
<tr>
<td>Protocol iso, MTU: 4470, Generation: 39, Route table: 0</td>
<td>Output packets: 83</td>
</tr>
<tr>
<td>Flags: None</td>
<td>Local statistics:</td>
</tr>
<tr>
<td>VCI 0.128</td>
<td>VCI 0.16</td>
</tr>
<tr>
<td>Flags: Active</td>
<td>Input bytes : 660</td>
</tr>
<tr>
<td>Total down time: 0 sec, Last down: Never</td>
<td>Output bytes : 5473</td>
</tr>
<tr>
<td>EPD threshold: 2129, Transmit weight cells: 10</td>
<td>Input packets: 11</td>
</tr>
<tr>
<td>ATM per-VC transmit statistics:</td>
<td>Output packets: 83</td>
</tr>
<tr>
<td>Tail queue packet drops: 0</td>
<td>ATM per-VC transmit statistics:</td>
</tr>
<tr>
<td>Traffic statistics:</td>
<td>Input bytes : 660</td>
</tr>
<tr>
<td>Input bytes : 0</td>
<td>Output bytes : 5473</td>
</tr>
<tr>
<td>Output bytes : 0</td>
<td>Input packets: 11</td>
</tr>
<tr>
<td>Input packets: 0</td>
<td>Output packets: 83</td>
</tr>
<tr>
<td>Output packets: 0</td>
<td>VCI 0.16</td>
</tr>
<tr>
<td>Flags: Active, ILMI</td>
<td>Total down time: 0 sec, Last down: Never</td>
</tr>
<tr>
<td>EPD threshold: 0, Transmit weight cells: 0</td>
<td>ATM per-VC transmit statistics:</td>
</tr>
</tbody>
</table>
Tail queue packet drops: 0
Traffic statistics:
Input bytes : 0
Output bytes : 4320
Input packets: 0
Output packets: 72

VCI 0.4
Flags: Active, OAM
OAM, Period 30 sec, Up count: 10, Down count: 10
Total down time: 0 sec, Last down: Never
EPD threshold: 2129, Transmit weight cells: 0

ATM per-VC transmit statistics:
Tail queue packet drops: 0
Traffic statistics:
Input bytes : 572
Output bytes : 572
Input packets: 11
Output packets: 11

OAM F4 cell statistics:
Total received: 11, Total sent: 11
Loopback received: 11, Loopback sent: 11
Last received: 00:00:18, Last sent: 00:00:18
RDI received: 0, RDI sent: 0
AIS received: 0, AIS sent: 0
show interfaces (Channelized DS3-to-DS0)

Syntax

```
show interfaces ds-fpc/pic/port:t1channel:ds0channel
<brief | detail | extensive>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized DS3-to-DS0 interface.

Options

```
ds-fpc/pic/port:t1channel:ds0channel—Display standard information about the specified channelized DS3-to-DS0 interface.

brief | detail | extensive—(Optional) Display the specified level of output interface.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.
```

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Channelized DS3-to-DS0) on page 1288

Output Fields

Table 34 on page 1280 lists the output fields for the show interfaces (all Channelized DS3 interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 34: Channelized DS3 show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface’s index number, which reflects its initialization sequence.</td>
<td>detail extensive, none</td>
</tr>
</tbody>
</table>
Table 34: Channelized DS3 show 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>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether C-bit parity mode or M13 mode is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>Physical layer framing format used on the link. It can be ESF or SF. The default is ESF.</td>
<td>All levels</td>
</tr>
<tr>
<td>Parent</td>
<td>(Channelized IQ interfaces only) Name and interface index of the interface to which a particular child interface belongs. None indicates that this interface is the top level.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>* interval seconds*—The time in seconds between successive keepalive requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* down-count number*—The number of keepalive packets that a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* up-count number*—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 34: Channelized DS3 show 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>Keepalive statistics</td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input</td>
<td>Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td>(last seen 00:00:00 ago)</td>
<td>Time since the last keepalive packet was received, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td>(last seen 00:00:00 ago)</td>
<td>Time since the last keepalive packet was sent, in the format hh:mm:ss.</td>
<td></td>
</tr>
</tbody>
</table>

LMI settings | (Frame Relay) Settings for Local Management Interface (LMI) can be either ANSI LMI settings or ITU LMI settings. ANSI LMI settings is the default. The format is (ANSI or ITU) LMI settings: value, value, value..., xx seconds, where value can be: | detail extensive none |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>n391dte</td>
<td>DTE full status polling interval (1–255)</td>
<td></td>
</tr>
<tr>
<td>n392dce</td>
<td>DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td>n392dte</td>
<td>DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td>n393dce</td>
<td>DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td>n393dte</td>
<td>DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td>t391dte</td>
<td>DTE polling timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td>t392dce</td>
<td>DCE polling verification timer (5–30 seconds)</td>
<td></td>
</tr>
</tbody>
</table>

LMI | (Frame Relay) LMI packet statistics: | detail extensive none |

| Input         | Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input: nn (last seen hh:mm:ss ago). |                 |
| Output        | Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output: nn (last seen hh:mm:ss ago). |                 |

LCP state | (PPP) Link Control Protocol state. | detail extensive none |
| Conf-ack-received | Acknowledgement was received. |                 |
| Conf-ack-sent | Acknowledgement was sent. |                 |
| Conf-req-sent | Request was sent. |                 |
| Down        | LCP negotiation is incomplete (not yet completed or has failed). |                 |
| Not-configured | LCP is not configured on the interface. |                 |
| Opened      | LCP negotiation is successful. |                 |

NCP state | (PPP) Network Control Protocol state. | detail extensive none |
| Conf-ack-received | Acknowledgement was received. |                 |
| Conf-ack-sent | Acknowledgement was sent. |                 |
| Conf-req-sent | Request was sent. |                 |
| Down        | NCP negotiation is incomplete (not yet completed or has failed). |                 |
| Not-configured | NCP is not configured on the interface. |                 |
| Opened      | NCP negotiation is successful. |                 |
### Table 34: Channelized DS3 show 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><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-received</strong>—Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-sent</strong>—Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-received</strong>—Response was received for the challenge sent, but CHAP has not yet moved into the <strong>Success</strong> state. (Most likely with RADIUS authentication).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-sent</strong>—Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failure</strong>—CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: <strong>year-month-day hour:minute:second timezone hh:mm:ss ago</strong>. For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes, Output bytes</strong>—Number of bytes received and transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets, Output packets</strong>—Number of packets received and transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 34: Channelized DS3 show 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><strong>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td><strong>Drops</strong></td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>Framing errors</strong></td>
<td>Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td><strong>Giants</strong></td>
<td>Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td><strong>Runts</strong></td>
<td>Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td><strong>Policed discards</strong></td>
<td>Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td><strong>L3 incompletes</strong></td>
<td>Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td><strong>L2 channel errors</strong></td>
<td>Counter increments when the software could not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td><strong>L2 mismatch timeouts</strong></td>
<td>Count of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td><strong>SRAM errors</strong></td>
<td>Number of hardware errors that occurred in the static RAM (SRAM) on the PIC. If the value in this field increments, the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td><strong>HS link CRC errors</strong></td>
<td>Count of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Carrier transitions</strong></td>
<td>Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly, (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td><strong>Drops</strong></td>
<td>Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>Aged packets</strong></td>
<td>Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></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><strong>DS1 alarms</strong></td>
<td>Media-specific defects that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>DS1 defects</strong></td>
<td>• LOS—Loss of signal. • LOF—Loss of frame. • AIS—Alarm indication signal. • YLW—Yellow alarm. Indicates errors at the remote site receiver.</td>
<td></td>
</tr>
<tr>
<td><strong>T1 media</strong></td>
<td>Counts of T1 media-specific errors.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
</tbody>
</table>

The T1 media-specific error types can be:

- **SEF**—Severely errored framing
- **BEE**—Bit error event
- **AIS**—Alarm indication signal
- **LOF**—Loss of frame
- **LOS**—Loss of signal
- **YELLOW**—Errors at the remote site receiver
- **BPV**—Bipolar violation
- **EXZ**—Excessive zeros
- **LCV**—Line code violation
- **PCV**—Pulse code violation
- **CS**—Carrier state
- **LES**—Line error seconds
- **ES**—Errored seconds
- **SEFS**—Severely errored framing seconds (section)
- **SES**—Severely errored seconds
- **BES**—Bit error seconds
- **UAS**—Unavailable seconds
### Table 34: Channelized DS3 show 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><strong>DS3 media</strong></td>
<td>Counts of T3 media-specific errors. For detailed definitions of the T3 (DS-3) error events (BPV, EXZ, LCV, PCV, and CCV) and performance parameters (LES, PES, PSES, CES, CSES, SEFS, and UAS), see RFC 2496.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• PLL Lock—Phase-locked loop out of lock</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reframing—Frame alignment recovery time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS—Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOF—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOS—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IDLE—Idle code detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• YELLOW—Remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BPV—Bipolar violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EXZ—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LCV—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PCV—Pulse code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CCV—C-bit coding violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LES—Line error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PES—P-bit errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PSES—P-bit errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CES—C-bit errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CSES—C-bit severely errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SEFS—Severely errored framing seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UAS—Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td><strong>HDLC configuration</strong></td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Giant threshold—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runt threshold—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeslots—Configured timeslots for the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byte encoding—Byte encoding used: <strong>Nx64K</strong> or <strong>Nx56K</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data inversion—HDLC data inversion setting: <strong>Enabled</strong> or <strong>Disabled</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Interface transmit queues</strong></td>
<td>Name of the transmit queues and their associated statistics for each DS1 channel on the Channelized DS3-to-DS1 PIC.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• B/W—Queue bandwidth as a percentage of the total interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WRR—Weighted round-robin (in percent).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bytes—Number of bytes transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors—Number of packet errors.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 34: Channelized DS3 show 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><strong>DS1 or DS3 BERT configuration</strong></td>
<td><strong>BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</strong></td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>BERT time period</strong>—Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Elapsed</strong>—Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Induced error rate</strong>—Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Algorithm</strong>—Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
</tbody>
</table>
| **Packet Forwarding Engine configuration** | Information about the configuration of the Packet Forwarding Engine:  
• **Destination slot**—FPC slot number.  
• **PLP byte**—Packet Level Protocol byte.                                                                 | extensive |
| **CoS information**               | Information about the CoS queue for the physical interface.                                                                                           | extensive |
|                                   | • **CoS transmit queue**—Queue number and its associated user-configured forwarding class name.                                                         |                 |
|                                   | • **Bandwidth %**—Percentage of bandwidth allocated to the queue.                                                                                     |                 |
|                                   | • **Bandwidth bps**—Bandwidth allocated to the queue (in bps).                                                                                         |                 |
|                                   | • **Buffer %**—Percentage of buffer space allocated to the queue.                                                                                      |                 |
|                                   | • **Buffer usec**—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time. |                 |
|                                   | • **Priority**—Queue priority: low or high.                                                                                                             |                 |
|                                   | • **Limit**—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available. |                 |
| **Logical Interface**             |                                                                                                                                                    |                 |
| **Logical interface**             | Name of the logical interface.                                                                                                                        | All levels     |
| **Index**                         | Logical interface index number, which reflects its initialization sequence.                                                                           | detail extensive none |
| **SNMP ifIndex**                  | Logical interface SNMP interface index number.                                                                                                       | detail extensive none |
| **Generation**                    | Unique number for use by Juniper Networks technical support only.                                                                                     | detail extensive |
| **Flags**                         | Information about the logical interface; values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152. | All levels     |
| **Encapsulation**                 | Encapsulation on the logical interface.                                                                                                               | All levels     |
| **Bandwidth**                     | Bandwidth configured on the interface.                                                                                                                | All levels     |
| **Protocol**                      | Protocol family configured on the logical interface, such as iso, inet6, mpls.                                                                       | detail extensive none |
Table 34: Channelized DS3 show 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>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Redundant Link</td>
<td>(LSQ redundancy) Backup link for Link Services IQ redundancy.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces extensive (Channelized DS3-to-DS0)

```
user@host> show interfaces ds-0/0/0:0:0:0 extensive

Physical interface: ds-0/0/0:0:0, Enabled, Physical link is Up
  Interface index: 174, SNMP ifIndex: 4298, Generation: 177
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: 640kbps, FCS: 16,
    Mode: C/Bit parity, Framing: ESF
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Hold-times     : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input : 280 (last seen 00:00:09 ago)
    Output: 286 (last sent 00:00:00 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
    mpls: Not-configured
  CHAP state: Not-configured
  Last flapped  : 2002-05-23 17:53:29 PDT (00:46:46 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes :  6814 16 bps
```
Output bytes: 28840          72 bps
Input packets:  568           0pps
Output packets:  893           0pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 39, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 2, L2 mismatch timeouts: 0,
  HS link CRC errors: 0
Output errors:
  Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0
DS1 alarms: None
DS3 alarms: None
DS1 defects: None
DS3 defects: None

T1 media:  Seconds  Count  State
  SEF        0        0   OK
  BEE        5        1   OK
  AIS        0        0   OK
  LOF        0        0   OK
  LOS        0        0   OK
  YELLOW     17       1   OK
  BPV        0        0
  EXZ        0        0
  LCV        5       27765
  PCV        0        0
  CS         0        0
  LES        0
  ES         0
  SES        5
  SEFS       10
  BES        0
  UAS        0

DS3 media:  Seconds  Count  State
  PLL Lock    0        0   OK
  Reframing   0        0   OK
  AIS         0        0   OK
  LOF         0        0   OK
  LOS         0        0   OK
  IDLE        0
  YELLOW     0        0   OK
  BPV        1       65535
  EXZ        1       65535
  LCV        2      131070
  PCV        1        1825
  CCV        0
  LES        1
  PES        1
  PSES       1
  CES        0
  CSES       0
  SEFS       0
  UAS        0

Interface transmit queues:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Packets</th>
<th>Bytes</th>
<th>Drops</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue0</td>
<td>95</td>
<td>95</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Queue1</td>
<td>5</td>
<td>5</td>
<td>893</td>
<td>28840</td>
<td>0</td>
</tr>
</tbody>
</table>

HDLGC configuration:
  Giant threshold: 1514, Runt threshold: 3
  Timeslots: 1-10
  Byte encoding: Nx64K, Data inversion: Disabled

DS3 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Algorithm: $2^{15} - 1$, Induced error rate: $10^{-0}$
DS1 BERT configuration:
  BERT time period: 10 seconds, Elapsed: 0 seconds
  Induced Error rate: $10^{-0}$, Algorithm: $2^{15} - 1$, $0.151$, Pseudorandom (9)
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 2 (0x01)
CoS information:  

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Limit</td>
<td>% bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>608000</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>32000</td>
</tr>
</tbody>
</table>

Logical interface ds-0/0/0:0:0.0 (Index 5) (SNMP ifIndex 4299) (Generation 943)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol inet, MTU: 1500, Generation: 949, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast:

198.51.100.255,
  Generation: 1849
show interfaces (Channelized DS3-to-DS1)

Syntax

show interfaces t1-fpc/pic/port:t1channel
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized DS3-to-DS1 interface.

Options

 t1-fpc/pic/port:t1channel—Display standard information about the specified channelized DS3-to-DS1 interface.

 brief | detail | extensive | terse—(Optional) Display brief, detail, extensive, or terse information about the interface.

 descriptions—(Optional) Display interface description strings.

 media—(Optional) Display media-specific information about network interfaces.

 snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

 statistics—(Optional) Display static interface statistics.

Required Privilege

view

List of Sample Output

show interfaces extensive (channelized DS3-to-DS1) on page 1291

Output Fields

See the output field table for the show interfaces (Channelized DS3-to-DS0) command.

Sample Output

show interfaces extensive (channelized DS3-to-DS1)

user@host> show interfaces t1-0/0/0:0 extensive

Physical interface: t1-0/0/0:0, Enabled, Physical link is Up
  Interface index: 210, SNMP ifIndex: 14, Generation: 2977
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: 640kbps,
  Loopback: None, FCS: 16, Mode: C/Bit parity, Framing: ESF
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Hold-times     : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
- Input: 30 (last seen 00:00:05 ago)
- Output: 29 (last sent 00:00:00 ago)

LCP state: Opened
CHAP state: Not-configured
Last flapped: 2002-05-23 17:30:12 PDT (17:29:43 ago)
Statistics last cleared: Never

Traffic statistics:
- Input bytes: 944 (16 bps)
- Output bytes: 1162 (16 bps)
- Input packets: 66 (0 pps)
- Output packets: 82 (0 pps)

Input errors:
- Errors: 1, Drops: 0, Framing errors: 1, Policed discards: 8, L3 incompletes: 0, L2 channel errors: 1, L2 mismatch timeouts: 0, HS link CRC errors: 0, SRAM errors: 0

Output errors:
- Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0

T1 media:
- SEF: 0 seconds (0 OK)
- BEE: 11 seconds (5 OK)
- AIS: 28 seconds (1 OK)
- LOF: 27 seconds (1 OK)
- LOS: 0 seconds (0 OK)
- YELLOW: 23 seconds (1 OK)
- BPV: 0 seconds (0)
- EXZ: 0 seconds (0)
- LCV: 11 seconds (20574)
- PCV: 0 seconds (0)
- CS: 0 seconds (0)
- LES: 28 seconds (0)
- ES: 28 seconds (0)
- SES: 39 seconds (0)
- SEFS: 50 seconds (0)
- BES: 0 seconds (0)
- UAS: 0 seconds (0)

DS3 media:
- PLL Lock: 0 seconds (0 OK)
- Reframing: 0 seconds (0 OK)
- AIS: 0 seconds (0 OK)
- LOF: 1 second (1 OK)
- LOS: 1 second (1 OK)
- IDLE: 0 seconds (0 OK)
- YELLOW: 0 seconds (0 OK)
- BPV: 2 seconds (131070)
- EXZ: 3 seconds (49910)
- LCV: 5 seconds (180980)
- PCV: 2 seconds (327)
- CCV: 12 seconds (264558)
- LES: 3 seconds (0)
- PES: 3 seconds (0)
- PSES: 2 seconds (0)
- CES: 13 seconds (0)
- CSES: 13 seconds (0)
SEFS                      1
UAS                      35

Interface transmit queues:

<table>
<thead>
<tr>
<th>Queue</th>
<th>B/W</th>
<th>WRR</th>
<th>Packets</th>
<th>Bytes</th>
<th>Drops</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue0</td>
<td>95</td>
<td>95</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Queue1</td>
<td>5</td>
<td>5</td>
<td>82</td>
<td>1162</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

HDLC configuration:
Giant threshold: 1514, Runt threshold: 3
Timeslots: 1-10
Line encoding: B8ZS, Byte encoding: Nx64K, Data inversion: Disabled

DS3 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Algorithm: $2^{15} - 1$, Induced error rate: $10^{-0}$

DS1 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: $10^{-0}$, Algorithm: $2^{15} - 1$, 0.151, Pseudorandom (9)

Packet Forwarding Engine configuration:
Destination slot: 0, PLP byte: 2 (0x00) CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>95 bps</td>
<td>608000 usec</td>
<td>low</td>
</tr>
<tr>
<td>network-control</td>
<td>5 bps</td>
<td>32000 usec</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface t1-0/0/0 (Index 11) (SNMP ifIndex 23) (Generation 497)
Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
Bandwidth: 0
Protocol inet, MTU: 1500, Generation: 576, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255
Generation: 977
show interfaces (Channelized E1 IQ)

Syntax

```
show interfaces (ce1-fpc/pic/port | type-fpc/pic/port <channel>)
<brief | detail | extensive | terse></brie
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized E1 IQ interface.

Options

```
type-fpc/pic/port:<channel>—Interface type with optional corresponding channel levels. For the physical channelized E1 IQ interface, type is ce. For the clear channel, type is e1. At the first level of channelization, type is ds.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.
```

Required Privilege

view

List of Sample Output

- `show interfaces (Channelized E1 IQ) (Physical)` on page 1294
- `show interfaces extensive (Channelized E1 IQ Multilink PPP Encapsulation)` on page 1295
- `show interfaces extensive (Channelized E1 IQ MLFR Encapsulation)` on page 1296
- `show interfaces detail (Clear Channel E1)` on page 1297

Output Fields

For information about output fields, see the output field table for the `show interfaces (Channelized E1)` command. Output fields are listed in the approximate order in which they appear.

Sample Output

```
show interfaces (Channelized E1 IQ) (Physical)

user@host> show interfaces ce1-1/2/3

Physical interface: ce1-1/2/3, Enabled, Physical link is Up
Interface index: 18, SNMP ifIndex: 1128
```

Link-level type: Frame-relay, Controller, MTU: 1504, Clocking: Internal, Speed: E1, Loopback: None, FCS: 16, Framing: G704, Parent: None
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
DTE statistics:
  Enquiries sent : 43186
  Full enquiries sent : 8515
  Enquiry responses received : 43185
  Full enquiry responses received : 8515
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0
Nonmatching DCE-end DLCIs:
  2
Last flapped : 2002-10-04 17:52:51 PDT (00:32:57 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
DS1 alarms : None
DS1 defects : None

show interfaces extensive (Channelized E1 IQ Multilink PPP Encapsulation)

user@host> show interfaces ds-0/3/4:1 extensive

Physical interface: ds-0/3/4:1, Enabled, Physical link is Up
  Interface index: 151, SNMP ifIndex: 63, Generation: 34
  Link-level type: Multilink-PPP, MTU: 1518, Clocking: Internal, Speed: 64kbps,
  Loopback: None, FCS: 16,
  Parent: ce1-0/3/4 Interface index 150
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : None
  Hold-times : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input : 0 (last seen: never)
    Output: 0 (last sent: never)
  LCP state: Down
  CHAP state: Closed
  CoS queues : 4 supported, 4 maximum usable queues
  Last flapped : Never
  Statistics last cleared: 2005-12-21 10:32:15 PST (1w0d 03:10 ago)
  Traffic statistics:
    Input bytes : 0
    Output bytes : 6070570
    Input packets: 0
    Output packets: 209330
    Input errors:
      Errors: 3, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
      Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0,
L2 mismatch timeouts: 0, HS link CRC errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0, Resource errors: 0
HDLHC configuration:
  Giant threshold: 1528, Runt threshold: 2
  Timeslots : 1
  Data inversion: Disabled, Idle cycle flag: flags, Start end flag: shared
DS0 BERT configuration:
  BERT time period: 10 seconds, Elapsed: 0 seconds
  Induced Error rate: 10e-0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 4 (0x00)
Logical interface ds-0/3/4:1.0 (Index 74) (SNMP ifIndex 64) (Generation 13)
  Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol mlppp, Multilink bundle: 1s-0/1/0.0, MTU: 1514, Generation: 24, Route table: 0

show interfaces extensive (Channelized E1 IQ MLFR Encapsulation)

user@host> show interfaces ds-0/3/4:5 extensive

Physical interface: ds-0/3/4:5, Enabled, Physical link is Up
  Interface index: 155, SNMP ifIndex: 72, Generation: 38
  Link-level type: Multilink-FR, MTU: 1518, Clocking: Internal, Speed: 64kbps, Loopback: None, FCS: 16,
  Parent: cel-0/3/4 Interface index 150
  Device flags : Present Running
  Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : No-Keepalives DCE
  Hold-times : Up 0 ms, Down 0 ms
  ANSI LMI settings: n392dce 3, n393dce 4, t392dce 15 seconds
  LMI statistics:
    Input : 0 (last seen: never)
    Output: 0 (last sent: never)

DTE statistics:
  Enquiries sent : 0
  Full enquiries sent : 0
  Enquiry responses received : 0
  Full enquiry responses received : 0

DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0

Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0

CoS queues : 4 supported, 4 maximum usable queues
  Last flapped : 2005-12-21 09:59:01 PST (1w0d 03:44 ago)
  Statistics last cleared: 2005-12-21 10:32:15 PST (1w0d 03:10 ago)

Traffic statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
  Input errors:
show interfaces detail (Clear Channel E1)

user@host> show interfaces e1-1/2/6 detail

Physical interface: e1-1/2/6, Enabled, Physical link is Up
Interface index: 89, SNMP ifIndex: 1278, Generation: 341
Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: E1, Loopback: None

Logical interface e1-1/2/6.0 (Index 52) (SNMP ifIndex 1279) (Generation 169)
  Flags: Point-To-Point SNPP-Traps Encapsulation: PPP
  Bandwidth: 0

Errors: 3, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, L3 completes: 0, L2 channel errors: 0,
L2 mismatch timeouts: 0, HS link CRC errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
  Resource errors: 0
HDLC configuration:
  Giant threshold: 1528, Run threshold: 2
  Timeslots: 5
  Data inversion: Disabled, Idle cycle flag: flags, Start end flag: shared
DSS BERT configuration:
  BERT time period: 10 seconds, Elapsed: 0 seconds
  Induced Error rate: 10^-6, Algorithm: 2^15 – 1, 0.151, Pseudorandom (9)
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 4 (0x01)
Logical interface ds-0/3/4:5.0 (Index 78) (SNMP ifIndex 73) (Generation 17)
  Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0pps
  Output packets: 0 0pps
Protocol mfr, Multilink bundle: ls-0/1/0.1, MTU: 1514, Generation: 28, Route
table: 0
DLCI 10
  Flags: Active
  Total down time: 0 sec, Last down: Never
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
DLCI statistics:
  Active DLCI :1  Inactive DLCI :0
show interfaces (Channelized E1)

Syntax

show interfaces ds-fpc/pic/port:ds0channel
  
  <brief | detail | extensive | terse>
  
  <descriptions>
  
  <media>
  
  <snmp-index snmp-index>
  
  <statistics>

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information the specified channelized E1 interface.

Options

ds-fpc/pic/port:ds0channel—Display standard information about the specified channelized E1 interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Channelized E1) on page 1307

Output Fields

Table 35 on page 1298 lists the output fields for the show interfaces (Channelized E1 and Channelized E1 IQ) command. Output fields are listed in the approximate order in which they appear.

Table 35: Channelized E1 and Channelized E1 IQ show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
### Table 35: Channelized E1 and Channelized E1 IQ show 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>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>Physical layer framing format used on the link. It can be G704, G704-NO-CRC4, or Unframed. The default is G704.</td>
<td>All levels</td>
</tr>
<tr>
<td>Parent</td>
<td>(Channelized E1 IQ interfaces only) Name and interface index of the interface to which a particular child interface belongs. None indicates that this interface is the top level.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>

- **Interval seconds**—Time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.
- **Down-count number**—Number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.
- **Up-count number**—Number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.
Table 35: Channelized E1 and Channelized E1 IQ show interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keepalive statistics</td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input</strong>—Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was received, in the format <code>hh:mm:ss</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output</strong>—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was sent, in the format <code>hh:mm:ss</code>.</td>
<td></td>
</tr>
<tr>
<td>LMI settings</td>
<td>(Frame Relay) Settings for link management can be either ANSI LMI settings or ITU LMI settings. ANSI LMI settings is the default. The format is <em>(ANSI or ITU)</em> <code>LMI settings: value, value... xx seconds</code>, where <em>value</em> can be:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• n391dte—DTE full status polling interval (1–255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dce—DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dte—DTE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dce—DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dte—DTE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t391dte—DTE polling timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t392dce—DCE polling verification timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td>LMI</td>
<td>(Frame Relay) Statistics about the link management.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input</strong>—Number of packets coming in on the interface <code>(nn)</code> and how much time has passed since the last packet arrived. The format is <code>Input: nn (last seen hh:mm:ss ago)</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output</strong>—Number of packets sent out on the interface <code>(nn)</code> and how much time has passed since the last packet was sent. The format is <code>Output: nn (last sent hh:mm:ss ago)</code></td>
<td></td>
</tr>
<tr>
<td>DTE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE):</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiries sent</strong>—Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiries sent</strong>—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiry responses received</strong>—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiry responses received</strong>—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>DCE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiries received</strong>—Number of enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiries received</strong>—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiry responses sent</strong>—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiry responses sent</strong>—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
</tbody>
</table>
Table 35: Channelized E1 and Channelized E1 IQ show 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><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown messages received</strong>—Number of received packets that do not fall into any category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Asynchronous updates received</strong>—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Out-of-sequence packets received</strong>—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Keepalive responses timed out</strong>—Number of keepalive responses that timed out when no LMI packet was reported from n392dte or n393dce intervals. (See LMI settings).</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay, displayed only from the DTE) Number of DLCIs configured from the DCE.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-received</strong>—Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-sent</strong>—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Opened</strong>—LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-received</strong>—Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-sent</strong>—Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-received</strong>—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-sent</strong>—Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failure</strong>—CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>CoS Queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Input Rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Output Rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 35: Channelized E1 and Channelized E1 IQ show 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><strong>Traffic statistics</strong></td>
<td>Number of bytes and packets received and transmitted on the physical interface.</td>
<td>detailed extensive</td>
</tr>
<tr>
<td>• Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Errors</td>
<td>Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td>• Drops</td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>• Framing errors</td>
<td>Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td>• Giants</td>
<td>Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td>• Runts</td>
<td>Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td>• Policed discards</td>
<td>Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td>• L3 incompletes</td>
<td>Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td>• L2 channel errors</td>
<td>Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td>• L2 mismatch timeouts</td>
<td>Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td>• HS link CRC errors</td>
<td>Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td>• Resource errors</td>
<td>Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 35: Channelized E1 and Channelized E1 IQ show 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><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), then either the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets larger than the MTU threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

- **DS1 alarms**
  - E1 media-specific defects that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. The following lists all possible alarms and defects. For complete explanations of most of these alarms and defects, see Bellcore Telcordia GR-499-CORE.
  - **LOS**—Loss of signal.
  - **LOF**—Loss of frame.
  - **AIS**—Alarm indication signal.
  - **YLW**—Yellow alarm. Indicates errors at the remote site receiver.
Table 35: Channelized E1 and Channelized E1 IQ show 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><strong>E1 media</strong></td>
<td>Active alarms and defects, plus counts of specific E1 errors with detailed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td><strong>HDLC configuration</strong></td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Giant threshold</strong>—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt threshold</strong>—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Timeslots</strong>—Configured time slots for the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Line encoding HDB3</strong>—Line encoding used.</td>
<td></td>
</tr>
<tr>
<td><strong>Interface transmit queues</strong></td>
<td>Names of the transmit queues and their associated statistics for each DS0 channel on the Channelized E1 to DS0 PIC.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>B/W</strong>—Queue bandwidth as a percentage of the total interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>WRR</strong>—Weighted round robin (in percent).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—Number of bytes transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Number of packet errors.</td>
<td></td>
</tr>
</tbody>
</table>
Table 35: Channelized E1 and Channelized E1 IQ show 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>DSx BERT configuration</td>
<td>DSx BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• BERT time period—Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Elapsed—Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Induced error rate—Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Algorithm—Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding Engine configuration</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Destination slot—FPC slot number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PLP byte—Packet Level Protocol byte.</td>
<td></td>
</tr>
<tr>
<td>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
</tbody>
</table>
Table 35: Channelized E1 and Channelized E1 IQ show 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>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the logical interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>(Frame Relay) Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than one second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>(Frame Relay) Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, mpls.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Multilink bundle</td>
<td>(Multilink) Interface name for the multilink bundle, if configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active—Set when the link is active and the DTE and DCE are exchanging information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Set when link is active, but no information is received from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unconfigured—Set when the corresponding DLCI in the DCE is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured—Set when the corresponding DLCI in the DCE is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dce-configured—Displayed when the command is issued from the DTE.</td>
<td></td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active DLCI—Number of active DLCIs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inactive DLCI—Number of inactive DLCIs.</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

show interfaces extensive (Channelized E1)

```
user@host> show interfaces ds-0/1/1:1 extensive

Physical interface: ds-0/1/1:1, Enabled, Physical link is Down
Interface index: 163, SNMP ifIndex: 37, Generation: 46
Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: E1,
Loopback: None, FCS: 16, Framing: G704
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 4 supported, 4 maximum usable queues
Last flapped : 2005-12-28 14:44:06 PST (00:00:30 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
  HS link CRC errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
    Resource errors: 0
DS1 alarms : LOF, LOS
DS1 defects : LOF, LOS
E1 media:
  SEF 982318 1 Defect Active
  BEE 0 0 OK
  AIS 0 0 OK
  LOF 982318 1 Defect Active
  LOS 982318 1 Defect Active
  YELLOW 0 0 OK
  BPV 1 1
  EXZ 1 1
  LCV 1 1
  PCV 1 2
  CS 0 0
  FEBE 1 9
  LES 1
  ES 982318
  SES 982318
  SEFS 982318
  BES 1
  UAS 0
Interface transmit queues:
  B/W WRR Packets Bytes Drops Errors
  Queue0 95 95 0 0 0 0
  Queue1 5 5 0 0 0 0
HDLC configuration:
  Giant threshold: 1514, Runt threshold: 3
  Timeslots : 31
  Line encoding: HDB3, Data inversion: Disabled, Idle cycle flag: flags,
  Start end flag: shared
DS1 BERT configuration:
```
BERT time period: 0 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^11 - 1, 0.152 and 0.153 (2047 type),
Pseudorandom (8)
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 2 (0x1b)

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer usec</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>95</td>
<td>low</td>
<td>none</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>0</td>
<td>low</td>
<td>none</td>
</tr>
</tbody>
</table>
show interfaces (Channelized OC12 IQ and IQE)

**Syntax**  
```
show interfaces (type-fpc/pic/port:<channel>:<channel>:<channel>)
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

**Release Information**  
Command introduced before Junos OS Release 7.4.

**Description**  
Display status information about the specified channelized OC12 IQ and IQE interface.

**Options**  
`type-fpc/pic/port:channel:channel:channel`—Interface type with optional corresponding channel levels.

For SONET mode, the interface type can be one of the following:

- `type-fpc/pic/port`—For the physical channelized OC12 IQ or IQE interface, **type** is `coc12`. For the clear channel, **type** is `so` (for OC12).
- `type-fpc/pic/port:channel`—At the first level of channelization, **type** can be `coc1` (channelized OC1), `ct3` (from `coc1`), `so` (for OC3), or `t3`.
- `type-fpc/pic/port:channel:channel`—At the second level of channelization, **type** can be `ct1` (from `ct3` or `coc1`) or `t1` (from `ct3` or `coc1`).
- `type-fpc/pic/port:channel:channel:channel`—At the third level of channelization, **type** is `ds` (from `ct1`).

For SDH mode, the interface type can be one of the following:

- `type-fpc/pic/port`—For the physical channelized OC12 IQ or IQE interface, **type** is `cstm4`. For the clear channel, **type** is `so` (for SONET/SDH (vc-4-4c)).
- `type-fpc/pic/port:channel`—At the first level of channelization, **type** can be `so` (from `cstm4`) or `cau4` (from `cstm4`).
- `type-fpc/pic/port:channel:channel`—At the second level of channelization, **type** can be `ct3` or `t3` (from or `cau4`).
- `type-fpc/pic/port:channel:channel:channel`—At the third level of channelization, **type** is `ct1` or `t1` (from `ct3`).
- `type-fpc/pic/port:channel:channel:channel:channel`—At the fourth level of channelization, **type** is `ds` (from `ct1`).

**brief | detail | extensive | terse**—(Optional) Display the specified level of output.

**descriptions**—(Optional) Display interface description strings.

**media**—(Optional) Display media-specific information about network interfaces.
snmp-index — (Optional) Display information for the specified SNMP index of the interface.

statistics — (Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces extensive (CAU4 on Channelized OC-12 IQ) on page 1310
show interfaces extensive (Channelized OC1 on Channelized OC12 IQ) on page 1310
show interfaces extensive (Channelized OC12 IQ) (Physical) on page 1310
show interfaces extensive (Channelized T1 from Channelized OC12 IQ) on page 1311
show interfaces extensive (Channelized T3 on Channelized OC12 IQ) on page 1311
show interfaces extensive (CSTM4 on Channelized OC-12 IQ) on page 1311
show interfaces extensive (DS0 on Channelized OC12 IQ) on page 1311
show interfaces extensive (SONET Interface on Channelized OC12 IQ) on page 1312
show interfaces extensive (T1 on Channelized OC12 IQ) on page 1312

Output Fields

See the output field table for the show interfaces (Channelized OC3 IQ and IQE) command.

Sample Output

show interfaces extensive (CAU4 on Channelized OC-12 IQ)

user@host> show interfaces cau4-0/2/0:1 extensive

Physical interface: cau4-0/2/0:1, Enabled, Physical link is Up
  Interface index: 219, SNMP ifIndex: 139, Generation: 221
  Link-level type: Controller, Clocking: Internal, SDH mode, Speed: OC3, Loopback: None, Parent: cstm4-0/2/0 Interface index 216
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : None
  ...

show interfaces extensive (Channelized OC1 on Channelized OC12 IQ)

user@host> show interfaces extensive coc1-4/2/0:7

Physical interface: coc1-4/2/0:7, Enabled, Physical link is Up
  Interface index: 281, SNMP ifIndex: 2524, Generation: 728
  Link-level type: Controller, MTU: 4474, Clocking: Internal, SONET mode, Speed: 51840kbps, Loopback: None, FCS: 16, Payload scrambler: Disabled, Parent: coc12-4/2/0 (Index 266)
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags : None
  ...

show interfaces extensive (Channelized OC12 IQ) (Physical)

user@host> show interfaces extensive coc12-4/2/0
show interfaces extensive (Channelized T1 from Channelized OC12 IQ)

user@host> show interfaces extensive ct1-4/2/0:7:1

Physical interface: ct1-4/2/0:4:1, Enabled, Physical link is Up
  Interface index: 305, SNMP ifIndex: 2410, Generation: 640
  Link-level type: Controller, MTU: 1504, Clocking: Internal, Speed: T1,
  Loopback: None, FCS: 16,
  Framing: ESF, Parent: coc1-4/2/0:7 (Index 304)
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags : None
...
show interfaces extensive (SONET Interface on Channelized OC12 IQ)

```
user@host>  show interfaces so-0/2/0:1 extensive
  Physical interface: so-0/2/0:1, Enabled, Physical link is Up
  Interface index: 750, SNMP ifIndex: 23, Generation: 11709
  Link-level type: Multilink-FR, MTU: 4474, Clocking: Internal, SONET mode,
  Speed: OC3, Loopback: None, FCS: 16,
  Payload scrambler: Enabled, Parent: coc12-0/2/0 Interface index 749
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : Keepalives DTE
```

show interfaces extensive (T1 on Channelized OC12 IQ)

```
user@host>  show interfaces t1-0/2/0:1:1:1 extensive
  Physical interface: t1-0/2/0:1:1, Enabled, Physical link is Up
  Interface index: 222, SNMP ifIndex: 143, Generation: 226
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: T1,
  Loopback: None, FCS: 16, Framing: ESF, Parent: ct3-0/2/0:1 Interface index 221
  Interface index 221
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : Keepalives
```

Copyright © 2019, Juniper Networks, Inc.
show interfaces (Channelized OC12)

Syntax

```
show interfaces t3-fpc/pic/port:t3channel
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display status information about the specified channelized OC12 interface.

Options

```
t3-fpc/pic/port:t3channel—Display standard information about the specified channelized OC12 interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.
```

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Channelized OC12) on page 1313

Output Fields

See the output field table for the `show interfaces (Channelized OC3 IQ and IQE)` command.

Sample Output

```
show interfaces extensive t3-0/3/0:0 extensive

Physical interface: t3-0/3/0:0, Enabled, Physical link is Up
  Interface index: 32, SNMP ifIndex: 21, Generation: 2719
  Link-level type: Frame-Relay, PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: T3, Loopback: None, SONET Loopback: None, FCS: 16, Mode: C/Bit parity
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalive DTE
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
  DTE statistics:
```
Enquiries sent                     : 43186
Full enquiries sent                : 8515
Enquiry responses received         : 43185
Full enquiry responses received    : 8515

DCE statistics:
Enquiries received                 : 0
Full enquiries received            : 0
Enquiry responses sent             : 0
Full enquiry responses sent        : 0

Common statistics:
Unknown messages received          : 0
Asynchronous updates received      : 0
Out-of-sequence packets received   : 0
Keepalive responses timedout       : 0

Nonmatching DCE-end DLCIs:
  2

Hold-times : Up 0 ms, Down 0 ms

Statistics last cleared: Never

Traffic statistics:
Input bytes : 1700 0 bps
Output bytes : 1714 0 bps
Input packets: 123 0 pps
Output packets: 124 0 pps

Input errors:
  Errors: 0, Drops: 0, Framing errors: 1100817, Bucket drops: 0,
  Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0,
  L2 mismatch timeouts: 0, HS link CRC errors: 0, SRAM errors: 0

Output errors:
  Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0

DS3 alarms : None
SONET alarms : None
DS3 defects : None
SONET defects : None

DS3 media:

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>18</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>IDLE</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>YELLOW</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BPV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EXZ</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LCV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PCV</td>
<td>36</td>
<td>122399</td>
<td></td>
</tr>
<tr>
<td>CCV</td>
<td>72</td>
<td>91948</td>
<td></td>
</tr>
<tr>
<td>LES</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PES</td>
<td>18</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PSES</td>
<td>18</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>CES</td>
<td>18</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CSES</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEFS</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

HDLC configuration:
Policing bucket: Disabled
Shaping bucket : Disabled
Giant threshold: 4484, Runt threshold: 3

DSU configuration:
Compatibility mode: None, Scrambling: Disabled, Subrate: Disabled
FEAC loopback: Inactive, Response: Disabled, Count: 0

DS3 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Algorithm: Unknown (0), Induced error rate: 10e-0

Interface transmit queues:

<table>
<thead>
<tr>
<th>Queue</th>
<th>B/W</th>
<th>WRR</th>
<th>Packets</th>
<th>Bytes</th>
<th>Drops</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue0</td>
<td>95</td>
<td>95</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Queue1</td>
<td>5</td>
<td>5</td>
<td>529</td>
<td>6348</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SONET PHY:

<table>
<thead>
<tr>
<th>PLL Lock</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHY Light</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>20</td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

SONET section:

<table>
<thead>
<tr>
<th>BIP-B1</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SEF</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOS</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOF</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ES-S</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SES-S</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SEFS-S</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SONET line:

<table>
<thead>
<tr>
<th>BIP-B2</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REI-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RDI-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AIS-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BERR-SF</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BERR-SD</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ES-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SES-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UAS-L</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ES-LFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SES-LFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UAS-LFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SONET path:

<table>
<thead>
<tr>
<th>BIP-B3</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REI-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOP-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AIS-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RDI-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNEQ-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PLM-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ES-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SES-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UAS-P</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ES-PFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SES-PFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UAS-PFE</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Received SONET overhead:

- F1 : 0x00, J0 : 0x00, K1 : 0x00, K2 : 0x00
- S1 : 0x00, C2 : 0x04, C2(cmp) : 0x04, F2 : 0x00
- Z3 : 0x00, Z4 : 0x00, S1(cmp) : 0x00, V5 : 0x00
- V5(cmp) : 0x00

Transmitted SONET overhead:

- F1 : 0x00, J0 : 0x01, K1 : 0x00, K2 : 0x00
- S1 : 0x00, C2 : 0x04, F2 : 0x00, Z3 : 0x00
- Z4 : 0x00, V5 : 0x00

Received path trace: t3-0/3/0:0

- 74 33 2d 30 2f 33 2f 33 a 30 00 00 00 00 0d 0a t3-0/3/0:0......

Transmitted path trace: t3-0/3/0:0

- 74 33 2d 30 2f 33 2f 33 a 30 00 00 00 00 00 00 t3-0/3/0:0......

Packet Forwarding Engine configuration:

- Destination slot: 0, PLP byte: 1 (0x00)

CoS information:
<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>bps</td>
<td>%</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>42499200</td>
<td>95</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>2236800</td>
<td>5</td>
</tr>
</tbody>
</table>

Logical interface t3-0/3/0:0.0 (Index 11) (SNMP ifIndex 268) (Generation 499)
Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 4470, Generation: 578, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255,
  Generation: 98
DLCI 100
  Flags: Active, Dce-configured
  Total down time: 0 sec, Last down: Never
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
DLCI statistics:
  Active DLCI : 2 Inactive DLCI : 0
show interfaces (Channelized OC3 IQ and IQE)

 Syntax

 `show interfaces (type-fpc/pic/port <:channel>:<channel>:<channel>)`
 `<brief | detail | extensive | terse>`
 `<descriptions>`
 `<media>`
 `<snmp-index snmp-index>`
 `<statistics>`

 Release Information

 Command introduced before Junos OS Release 7.4.

 Description

 (M Series and T Series routers only) Display status information about the specified channelized OC3 IQ or IQE interface.

 Options

 `type-fpc/pic/port:channel:channel:channel`—Interface type with optional corresponding channel levels. The interface type can be one of the following:

 - `type-fpc/pic/port`—For the physical interface, `type` is `coc3`. For the clear channel, `type` is `so` (for OC3).

 - `type-fpc/pic/port:channel`—At the first level of channelization, `type` can be `coc1` (channelized OC1), `ct3` (from `coc1`), or `t3` (from `coc1`).

 - `type-fpc/pic/port:channel:channel`—At the second level of channelization, `type` can be `ct1` (from `coc1` or `ct3`) or `t1` (from `coc1` or `ct3`).

 - `type-fpc/pic/port:channel:channel:channel`—At the third level of channelization, `type` can be `ds` (from `ct1`).

 `brief | detail | extensive | terse`—(Optional) Display the specified level of output.

 `descriptions`—(Optional) Display interface description strings.

 `media`—(Optional) Display media-specific information about network interfaces.

 `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

 `statistics`—(Optional) Display static interface statistics.

 Required Privilege

 `view`

 List of Sample Output

 `show interfaces extensive (Channelized OC3 IQ) (Physical) on page 1331`
 `show interfaces extensive (Channelized OC1 on Channelized OC3 IQ) on page 1332`
 `show interfaces extensive (Channelized T1 on Channelized OC3 IQ) on page 1333`
 `show interfaces extensive (DS0 on Channelized OC3 IQ) on page 1334`
**Output Fields**  
Table 36 on page 1318 lists the output fields for the `show interfaces` (all Channelized OC interfaces) command. Output fields are listed in the approximate order in which they appear.

**Table 36: Channelized OC show interfaces Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Interface description.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Link-level type</strong></td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Clocking</strong></td>
<td>SONET/SDH reference clock source. It can be Internal or External. Clocking is configured and displayed only for channel 0.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Framing mode</strong></td>
<td>Framing mode: SONET or SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>SONET loopback</strong></td>
<td>Whether loopback is enabled on a SONET/SDH interface, and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>FCS</strong></td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16-bit.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Payload scrambler</strong></td>
<td>Whether payload scrambling is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Parent</strong></td>
<td>Name and interface index of the interface to which a particular child interface belongs. None indicates that this interface is the top level.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Device flags</strong></td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface flags</strong></td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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><strong>Link flags</strong></td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>ANSI or ITU LMI settings</strong></td>
<td>(Frame Relay) Settings for Local Management Interface (LMI). The format is (ANSI or ITU) LMI settings: value, value... nn seconds, where value can be:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• n391dte—DTE full status polling interval (1–255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dce—DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dte—DTE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dce—DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dte—DTE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t391dte—DTE polling timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t392dce—DCE polling verification timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td><strong>LMI statistics</strong></td>
<td>(Frame Relay) Statistics about the link management.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input—Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input: nn (last sent hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output: nn (last sent hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td><strong>DTE statistics</strong></td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE):</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Enquiries sent—Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiries sent—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses received—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses received—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td><strong>DCE statistics</strong></td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Enquiries received—Number of enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiries received—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses sent—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses sent—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown messages received</strong>—Number of received packets that do not fall into any category.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Asynchronous updates received</strong>—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Out-of-sequence packets received</strong>—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Keepalive responses timedout</strong>—Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay) Number of DLCIs configured from the DCE, displayed only from the DTE.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is <code>Last flapped: year-month-day hh:mm:ss timezone year-month-day (hh:mm:ss ago)</code>. For example, <code>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</code>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>CoS Queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>DS1 alarms</strong></td>
<td>E1 or T1 media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. See the following list for all possible alarms and defects. For complete explanations of most of these alarms and defects, see Bellcore Telcordia GR-499-CORE.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS</strong>—Alarm indication signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>YLW</strong>—Yellow alarm. Indicates errors at the remote site receiver.</td>
<td></td>
</tr>
<tr>
<td><strong>DS1 defects</strong></td>
<td></td>
<td></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>T1 media</td>
<td>Counts of T1 or E1 media-specific errors.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The T1 or E1 media-specific error types are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>BEE</strong>—Bit error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>AIS</strong>—Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>YELLOW</strong>—Errors at the remote site receiver</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>BPV</strong>—Bipolar violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>EXZ</strong>—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LCV</strong>—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>PCV</strong>—Pulse code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>CS</strong>—Carrier state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>FEBE</strong>—Far-end block error (E1 only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LES</strong>—Line error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>ES</strong>—Errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>BES</strong>—Bit error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>SES</strong>—Severely errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>SEFS</strong>—Severely errored framing seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>UAS</strong>—Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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><strong>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>whose meaning might not be obvious:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bucket Drops</strong>—Drops caused by traffic load exceeding the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmit/receive leaky bucket configuration. The default is off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discarded because they were not recognized or not of interest. Usually, this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASICS responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SRAM errors</strong>—Number of hardware errors that occurred in the static RAM (SRAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PIC. If the value of this field increments, the PIC is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link FIFO overflows</strong>—Number of FIFO overflows on the high-speed links</td>
<td></td>
</tr>
<tr>
<td></td>
<td>between the ASICS responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Channelized OC show 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>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Carrier transitions — Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors — Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops — Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aged packets — Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HS link FIFO underflows — Number of FIFO underflows on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MTU errors — Number of packets whose size exceeds the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors — Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Egress queues</td>
<td>Total number of egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Queued packets — Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets — Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets — Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Active alarms</td>
<td>Defects that can prevent the interface from passing packets:</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Active defects</td>
<td>• None — There are no active defects or alarms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOF — Loss of frame.</td>
<td></td>
</tr>
<tr>
<td>SONET alarms</td>
<td>Media-specific defects that can prevent the interface from passing packets.</td>
<td>All levels</td>
</tr>
<tr>
<td>SONET defects</td>
<td>When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SONET PHY, SONET section, SONET line, and SONET path.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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><strong>SONET vt</strong></td>
<td>SONET virtual-tributary (VT) alarms and defects:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B2</strong>—Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-V</strong>—Remote error indication (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOP-V</strong>—Loss of pointer (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-V</strong>—Alarm indication signal (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-V</strong>—Remote defect indication (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UNEQ-V</strong>—Unequipped (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLM-V</strong>—Payload label mismatch (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-V</strong>—Errored seconds (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-V</strong>—Severely errored seconds (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-V</strong>—Unavailable seconds (near-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-VFE</strong>—Errored seconds (far-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-VFE</strong>—Severely errored seconds (far-end VT)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-VFE</strong>—Unavailable seconds (far-end VT)</td>
<td></td>
</tr>
<tr>
<td><strong>SONET PHY</strong></td>
<td>Counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLL Lock</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PHY Light</strong>—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td><strong>SONET section</strong></td>
<td>Counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B1</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOL</strong>—Loss of light</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-S</strong>—Errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-S</strong>—Severely errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEFS-S</strong>—Severely errored framing seconds (section)</td>
<td></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><strong>SONET line</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• State—State of the error. State other than OK indicates a problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• BIP-B2—Bit interleaved parity for SONET line overhead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• REI-L—Remote error indication (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RDI-L—Remote defect indication (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AIS-L—Alarm indication signal (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• BERR-SF—Bit error rate fault (signal failure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• BERR-SD—Bit error rate defect (signal degradation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ES-L—Errored seconds (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SES-L—Severely errored seconds (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UAS-L—Unavailable seconds (near-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ES-LFE—Errored seconds (far-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SES-LFE—Severely errored seconds (far-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UAS-LFE—Unavailable seconds (far-end line)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SONET path</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed information:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• State—State of the error. State other than OK indicates a problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• BIP-B3—Bit interleaved parity for SONET section overhead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• REI-P—Remote error indication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LOP-P—Loss of pointer (path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• AIS-P—Path alarm indication signal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RDI-P—Path remote defect indication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UNEQ-P—Path unequipped</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PLM-P—Path payload (signal) label mismatch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ES-P—Errored seconds (near-end STS path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SES-P—Severely errored seconds (near-end STS path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UAS-P—Unavailable seconds (near-end STS path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ES-PFE—Errored seconds (far-end STS path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• SES-PFE—Severely errored seconds (far-end STS path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• UAS-PFE—Unavailable seconds (far-end STS path)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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>Received SONET overhead</td>
<td>Values of the received and transmitted SONET/SDH overhead:</td>
<td>extensive</td>
</tr>
<tr>
<td>Transmitted SONET overhead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDH alarms</td>
<td>SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for</td>
<td>All levels</td>
</tr>
<tr>
<td>SDH defects</td>
<td>a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fields for possible alarms and defects: SDH PHY, SDH regenerator section, SDH multiplex section, and SDH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>path.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For controller based SONET PICs, the SDH alarms and SDH defects output in the <code>show interface coc3 extensive</code> command output only shows the section and line level defects. The path level defects can be found under the SONET (so) interface output.</td>
<td></td>
</tr>
<tr>
<td>SDH PHY</td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLL Lock</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PHY Light</strong>—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td>SDH regenerator section</td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RS-BIP8</strong>—24-bit BIP for multiplex section overhead (B2 bytes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>OOF</strong>—Out of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RS-ES</strong>—Errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RS-SES</strong>—Severely errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RS-SEFS</strong>—Severely errored framing seconds (regenerator section)</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Channelized OC show 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><strong>SDH multiplex section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-BIP24</strong>—8-bit BIP for high-order path overhead (B3 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-FEBE</strong>—Far-end block error (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-FERF</strong>—Far-end remote fail (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-AIS</strong>—alarm indication signal (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-ES</strong>—Errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-SES</strong>—Severely errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-UAS</strong>—Unavailable seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-ES-FE</strong>—Errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-SES-FE</strong>—Severely errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MS-UAS-FE</strong>—Unavailable seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td><strong>SDH path</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-BIP8</strong>—8-bit BIP for regenerator section overhead (B1 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FEBE</strong>—Far-end block error (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-LOP</strong>—Loss of pointer (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-AIS</strong>—High-order-path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FERF</strong>—Far-end remote fail (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UNEQ</strong>—Unequipped (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-PLM</strong>—Payload label mismatch (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES</strong>—Errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES</strong>—Severely errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS</strong>—Unavailable seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES-FE</strong>—Errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES-FE</strong>—Severely errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS-FE</strong>—Unavailable seconds (far-end high-order path)</td>
<td></td>
</tr>
</tbody>
</table>
**Table 36: Channelized OC show 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><strong>Received SDH overhead</strong></td>
<td>Values of the received and transmitted SONET overhead:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• C2—Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• F1—Section user channel byte. This byte is set aside for the purposes of users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• K1 and K2—These bytes are allocated for APS signaling for the protection of the multiplex section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• J0—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal. Used to transmit a 1-byte fixed-length string or a 16-byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S1—Synchronization status. The S1 byte is located in the first STS-1 of an STS-N.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Z3 and Z4—Allocated for future use.</td>
<td></td>
</tr>
<tr>
<td><strong>Transmitted SDH overhead</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Received path trace</strong></td>
<td>Channelized OC12 interfaces allow path trace bytes to be sent inband across the SONET/SDH link. The received path trace value is the message received from the router at the other end of the fiber. The transmitted path trace value is the message that this router transmits. This information is specific to each of the 12 channelized OC12 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Transmitted path trace</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DS3 media</strong></td>
<td>Counts of T3 media-specific errors. For detailed definitions of the T3 (DS-3) error events (BPV, EXZ, LCV, PCV, and CCV) and performance parameters (LES, PES, PSES, CES, CSES, SEFS, and UAS), see RFC 2496.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

The DS3 or E3 media-specific error types can be:

- **PLL Lock**—Phase-locked loop out of lock
- **Reframing**—Frame alignment recovery time
- **AIS**—Alarm indication signal
- **LOF**—Loss of frame
- **LOS**—Loss of signal
- **IDLE**—Idle code detected
- **YELLOW**—Errors at the remote site receiver
- **BPV**—Bipolar violation
- **EXZ**—Excessive zeros
- **LCV**—Line code violation
- **PCV**—(DS3 only) Pulse code violation
- **CCV**—(DS3 only) C-bit coding violation
- **FEBE**—(DS3 only) Far-end block error
- **LES**—Line error seconds
- **PES**—(DS3 only) P-bit errored seconds
- **PSES**—(DS3 only) P-bit errored seconds (section)
- **CES**—(DS3 only) C-bit errored seconds
- **CSES**—(DS3 only) C-bit severely errored seconds
- **SEFS**—Severely errored framing seconds
- **UAS**—Unavailable seconds
Table 36: Channelized OC show 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>HDLC configuration</td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Policing bucket—Configured state of the receiving policer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shaping bucket—Configured state of the transmitting shaper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Giant threshold—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runt threshold—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeslots—Configured time slots for the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Line encoding—Line encoding used. It is always HDB3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byte encoding—(T1 only) Byte encoding used: N×64K or N×56K.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Line encoding—Line encoding used. For T1, the value can be B8ZS or AMI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data inversion—HDLC data inversion setting: Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Idle cycle flag—Idle cycle flags.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Start end flag—Start and end flag.</td>
<td></td>
</tr>
<tr>
<td>Interface transmit queues</td>
<td>Name of the transmit queues and their associated statistics for each DS3 channel</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>on the Channelized OC12 PIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• B/W—Queue bandwidth as a percentage of the total interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WRR—Weighted round-robin (in percent).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bytes—Number of bytes transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors—Number of packet errors.</td>
<td></td>
</tr>
<tr>
<td>DSU configuration</td>
<td>Information about the DSU configuration. The last three lines (Bit count, Error</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>bit count, and LOS information) are displayed only if a BERT has ever been run</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Compatibility mode—CSU/DSU compatibility mode: None, Larscom, Kentrox, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Digital-Link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scrambling—Payload scrambling. It can be Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Subrate—Configured subrate setting. Applies only when Digital-Link compatibility mode is used. It can be Disabled or display units in kbps.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FEAC loopback—(T3) Whether a far-end alarm and control (FEAC) loopback is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active or Inactive. This feature is used to send alarm or status information from</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the far-end terminal back to the near-end terminal and to initiate T3 loopbacks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>at the far-end terminal from the near-end terminal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Response—Whether the FEAC signal is Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—Number of FEAC loopbacks.</td>
<td></td>
</tr>
<tr>
<td>BERT configuration</td>
<td>(DS interfaces) BERT (bit error rate test) checks the quality of the line. This</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>output appears only when a BERT is run on the interface.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• BERT time period—Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Elapsed—Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Induced error rate—Configured rate at which the bit errors are induced in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BERT pattern.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Algorithm—Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Channelized OC show 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>Packet Forwarding Engine configuration</td>
<td>Information about the configuration of the Packet Forwarding Engine: • <strong>Destinationslot</strong>—FPC slot number. • <strong>PLP byte</strong>—Packet Level Protocol byte.</td>
<td>extensive</td>
</tr>
<tr>
<td>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>CoS transmit queue</strong>—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth %</strong>—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth bps</strong>—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer %</strong>—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer usec</strong>—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Priority</strong>—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Limit</strong>—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

Logical Interface

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input rate</strong>—Rate of bits and packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output rate</strong>—Rate of bits and packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 36: Channelized OC show 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>Transit statistics</td>
<td>Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, or mpls.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Multilink bundle</td>
<td>(If the logical interface is configured as part of a multilink bundle.) Interface name for the multilink bundle.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following:</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show interfaces extensive (Channelized OC3 IQ) (Physical)

user@host> show interfaces extensive coc3-0/0/0
```
Physical interface: coc3-0/0/0, Enabled, Physical link is Down
Interface index: 128, SNMP ifIndex: 22, Generation: 11
Description: pink coc3-0/0/0
Link-level type: Controller, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, Parent: None
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
Link flags : None
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 4 supported
Statistics last cleared: Never
SONET alarms : PLL, LOS
SONET defects : PLL, LOF, LOS, SEF, AIS-L
SONET PHY:                  Seconds  Count  State
PLL Lock                   681767   1  PLL Lock Error
PHY Light                   0       0  OK
SONET section:
  BIP-B1                   0       0
  SEF                     681767   1  Defect Active
  LOS                     681767   1  Defect Active
  LOF                     681767   1  Defect Active
  ES-S                    681767
  SES-S                   681767
  SEFS-S                  681767
SONET line:
  BIP-B2                   0       0
  REI-L                    0       0
  RDI-L                    0       0  OK
  AIS-L                    681767   1  Defect Active
  BERR-SF                  0       0  OK
  BERR-SD                  0       0  OK
  ES-L                     681767
  SES-L                    681767
  UAS-L                    681757
  ES-LFE                   0
  SES-LFE                  0
  UAS-LFE                  0
Received SONET overhead:
  F1 : 0x00, J0 : 0x00, K1 : 0xff, K2 : 0xff
  S1 : 0xff
Transmitted SONET overhead:
  F1 : 0x00, J0 : 0x01, K1 : 0x00, K2 : 0x00
  S1 : 0x00

---

show interfaces extensive (Channelized OC1 on Channelized OC3 IQ)

user@host>  show interfaces extensive coc1-0/0/0:1

Physical interface: coc1-0/0/0:1, Enabled, Physical link is Down
Interface index: 133, SNMP ifIndex: 27, Generation: 16
Link-level type: Controller, Clocking: Internal, SONET mode, Speed: 51840kbps,
Loopback: None, Parent: coc3-0/0/0
Interface index 128
Device flags : Present Running Down 16384
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
Link flags : None
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 4 supported
show interfaces extensive (Channelized T1 on Channelized OC3 IQ)

user@host> show interfaces extensive ct1-0/0/0:1:1

Physical interface: ct1-0/0/0:1:1, Enabled, Physical link is Down
Interface index: 134, SNMP ifIndex: 62, Generation: 17
Link-level type: Controller, Clocking: Internal, Speed: T1, Loopback: None,
Framing: ESF, Parent: coc1-0/0/0:1 Interface index 133
Device flags : Present Running Down 16384
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
Link flags : None
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 4 supported
Last flapped : 2005-02-04 14:54:35 PST (00:00:18 ago)
Statistics last cleared: Never
DS1 alarms : None
DS1 defects : AIS, LOF
T1 media: Seconds Count State
SEF 1 1 OK
BEE 1 1 OK
AIS 18 1 Defect Active
LOF 18 1 Defect Active
LOS 0 0 OK
YELLOW 0 0 OK
BPV 0 0
EXZ 0 0
LCV 0 0
PCV 0 0
CS 0 0
LES 18
ES 18
SES 18
SEFS 18
BES 0
UAS 14

DS1 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)
SONET alarms : None
SONET defects : None
SONET vt:
  BIP-BIP2 0 0
  REI-V 0 0
  LOP-V 0 0 OK
  AIS-V 19 1 Defect Active
  RDI-V 19 1 Defect Active
  UNEQ-V 0 0 OK
  PLM-V 19 1 Defect Active
  ES-V 19
  SES-V 19
  UAS-V 9
  ES-VFE 0
  SES-VFE 0
  UAS-VFE 0

Received SONET overhead:
  V5 : 0x07, V5(cmp) : 0x02

Transmitted SONET overhead:
  V5 : 0x02

Packet Forwarding Engine configuration:
  Destination slot: 0 (0x00)
L2 mismatch timeouts: 0, HS link CRC errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0, Resource errors: 0
Queue counters:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

HDLC configuration:
  Giant threshold: 1514, Runt threshold: 2
  Timeslots: 1-5
  Byte encoding: Nx64K, Data inversion: Disabled, Idle cycle flag: flags, Start end flag: shared
DS0 BERT configuration:
  BERT time period: 10 seconds, Elapsed: 0 seconds
  Induced Error rate: 10e-0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 4 (0x00)
show interfaces (Channelized STM1 IQ)

Syntax

```
show interfaces (type-fpc/pic/port <channel><channel>)
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized STM1 IQ interface.

Options

```
type-fpc/pic/port:channel:channel—Interface type with optional corresponding channel levels. The interface type can be one of the following types:

  • type-fpc/pic/port:channel—For the physical channelized STM1 IQ interface, type is cstm1. For the clear channel, type is so. For channelization, the STM1 IQ interface must be converted to interface type cau4.

  • type-fpc/pic/port:channel—At the first level of channelization, type can be cel or e1 (clear channel or fractional channel from cau4).

  • type-fpc/pic/port:channel:channel—At the second level of channelization, type is ds (from cel).

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.
```

Required Privilege

view

List of Sample Output

- show interfaces (Channelized STMI IQ) (Physical) on page 1337
- show interfaces (Channelized AU-4) (Physical) on page 1337
- show interfaces (Channelized E1) (Physical) on page 1337
- show interfaces (DS) on page 1338

Output Fields

See the output field table for the show interfaces (Channelized STMI) command.
Sample Output

show interfaces (Channelized STM1 IQ) (Physical)

```
user@host> show interfaces cstm1-0/0/0

Physical interface: cstm1-0/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 35
Link-level type: Frame-relay, Controller, Clocking: Internal, SDH mode,
Speed: OC3, Loopback: None, Parent: None Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
DTE statistics:
  Enquiries sent : 43186
  Full enquiries sent : 8515
  Enquiry responses received : 43185
  Full enquiry responses received : 8515
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0
Nonmatching DCE-end DLCIs:
  2
Last flapped : 2003-02-06 15:01:56 PST (07:15:06 ago)
```

show interfaces (Channelized AU-4) (Physical)

```
user@host> show interfaces cau4-0/0/0

Physical interface: cau4-0/0/0, Enabled, Physical link is Up
Interface index: 147, SNMP ifIndex: 36
Link-level type: Controller, Clocking: Internal, SDH mode, Speed: OC3,
Loopback: None, Parent: cstm1-0/0/0 Interface index 146
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link flags : None
Last flapped : 2003-02-06 19:36:31 PST (02:40:42 ago)
SDH alarms : None
SDH defects : None
```

show interfaces (Channelized E1) (Physical)

```
user@host> show interfaces cel-0/0/0:11

Physical interface: cel-0/0/0:11, Enabled, Physical link is Up
Interface index: 169, SNMP ifIndex: 288
Link-level type: Frame-relay, Controller, Clocking: Internal, Speed: E1,
Loopback: None, Framing: G704, Parent: cau4-0/0/0 Interface index 146
Device flags : Present Running
```
Interface flags: Point-To-Point SNMP-Traps
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
DTE statistics:
  Enquiries sent : 43186
  Full enquiries sent : 8515
  Enquiry responses received : 43185
  Full enquiry responses received : 8515
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0
Nonmatching DCE-end DLCIs:
  2
  Last flapped : 2003-02-06 22:05:23 PST (00:13:45 ago)
DS1 alarms : None
DS1 defects : None
SDH alarms : None
SDH defects : None

show interfaces (DS)

user@host> show interfaces ds-0/0/0:11:1

Physical interface: ds-0/0/0:11:1, Enabled, Physical link is Up
  Interface index: 170, SNMP ifIndex: 289
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: 640kbps,
  Loopback: Illegal, FCS: 16, Parent: ce1-0/0/0:11 Interface index 169
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags : Keepalives
  CoS Queues: 8 maximum usable queues, 4 in use
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 0 (never)
  LCP state: Conf-req-sent
  Egress queues: 8 supported, 4 in use

Logical interface ds-0/0/0:11:1.0 (Index 77) (SNMP ifIndex 290)
  Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
  Bandwidth: 0
  Protocol inet, MTU: 1500
  Flags: Protocol-Down
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 10.134.1.0/30, Local: 10.134.1.1

DLCI 100
  Flags: Active, Dce-configured
  Total down time: 0 sec, Last down: Never
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
Output packets: 0
show interfaces (Channelized STM1)

Syntax

```
show interfaces e1-fpc/pic/port:e1channel
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized STM1 interface.

Options

```
e1-fpc/pic/port:e1channel—Display standard status information about the specified channelized STM1 interface.
brief | detail | extensive | terse—(Optional) Display the specified level of output.
descriptions—(Optional) Display interface description strings.
media—(Optional) Display media-specific information about network interfaces.
snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.
statistics—(Optional) Display static interface statistics.
```

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Channelized STM1, SDH) on page 1351

Output Fields

Table 37 on page 1340 lists the output fields for the `show interfaces` (all Channelized STM1 interfaces) command. Output fields are listed in the approximate order in which they appear.

**Table 37: Channelized STM1 show interfaces Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 37: Channelized STMI show 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>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>Physical layer framing format used on the link. It can be G704, G704-NO-CRC4, or Unframed. The default is G704.</td>
<td>All levels</td>
</tr>
<tr>
<td>Parent</td>
<td>(Channelized STMI IQ interfaces only) Name and interface index of the interface to which a particular child interface belongs. None indicates that this interface is the top level.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the &quot;Device Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the &quot;Interface Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the &quot;Link Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>detail extensive, none</td>
</tr>
</tbody>
</table>

- **interval** seconds—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.
- **down-count number**—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.
- **up-count number**—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.
## Table 37: Channelized STMI show 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>Keepalive statistics</td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input</strong>—Number of keepalive packets received by PPP.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was received, in the format <em>hh:mm:ss</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output</strong>—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was sent, in the format <em>hh:mm:ss</em>.</td>
<td></td>
</tr>
<tr>
<td>ANSI LMI settings</td>
<td>(Frame Relay) Local Management Interface settings. The format is <em>(ANSI or ITU) LMI settings: value, value ... xx seconds</em>, where value can be:</td>
<td>detail extensive</td>
</tr>
<tr>
<td>ITU LMI settings</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• n391dte—DTE full status polling interval (1-255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dce—DCE error threshold (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dte—DCE error threshold (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dce—DCE monitored event count (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dte—DCE monitored event count (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t391dte—DTE polling timer (5-30 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t392dce—DCE polling verification timer (5-30 seconds)</td>
<td></td>
</tr>
<tr>
<td>LMI</td>
<td>(Frame Relay) Statistics about the link management.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input</strong>—Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is <em>Input: nn (last seen hh:mm:ss ago)</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output</strong>—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is <em>Output: nn (last seen hh:mm:ss ago)</em>.</td>
<td></td>
</tr>
<tr>
<td>DTE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE):</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiries sent</strong>—Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiries sent</strong>—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiry responses received</strong>—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiry responses received</strong>—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>DCE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiries received</strong>—Number of enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiries received</strong>—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Enquiry responses sent</strong>—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full enquiry responses sent</strong>—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 37: Channelized STM1 show 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><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown messages received</strong>—Number of received packets that do not fall into any category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Asynchronous updates received</strong>—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Out-of-sequence packets received</strong>—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Keepalive responses timed out</strong>—Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay, displayed only from the DTE) Number of DLCIs configured from the DCE.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-received</strong>—Acknowledgment was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-sent</strong>—Acknowledgment was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Opened</strong>—LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-received</strong>—Acknowledgment was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-sent</strong>—Acknowledgment was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—NCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Opened</strong>—NCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-received</strong>—Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-sent</strong>—Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-received</strong>—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-sent</strong>—Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failure</strong>—CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
### Table 37: Channelized STM1 show 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>Statistics last</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>cleared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>were meaning might not be obvious:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discarded because they were not recognized or not of interest. Usually, this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompleted</strong>—Number of incoming packets discarded because they failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>H5 link CRC errors</strong>—Number of errors on the high-speed links between the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASICS responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SRAM errors</strong>—Number of hardware errors that occurred in the static RAM (SRAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PIC. If the value of this field increments, the PIC is malfunctioning.</td>
<td></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>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td>DS1 alarms</td>
<td>E1 media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. The following lists all possible alarms and defects. For complete explanations of most of these alarms and defects, see <em>Bellcore Telcordia GR-499-CORE</em>.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS</strong>—Alarm indication signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>YLW</strong>—Yellow alarm. Indicates errors at the remote site receiver.</td>
<td></td>
</tr>
<tr>
<td>SDH alarms</td>
<td>SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SDH PHY, SDH regenerator section, SDH multiplex section, and SDH path.</td>
<td>All levels</td>
</tr>
<tr>
<td>SDH defects</td>
<td><strong>NOTE:</strong> For controller-based SONET PICs, the SDH alarms and SDH defects output in the <code>show interface cstm1 extensive</code> command output only shows the section and line level defects. The path level defects can be found under the SONET (so) interface output.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 37: Channelized STM1 show 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><strong>E1 media</strong></td>
<td>Active alarms and defects, plus counts of specific E1 errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td><strong>Error types can be:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS</strong>—Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BEE</strong>—Bit error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BES</strong>—Bit error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BPV</strong>—Bipolar violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CS</strong>—Carrier state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES</strong>—Errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>EXZ</strong>—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FEBE</strong>—Far-end block error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LCV</strong>—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LES</strong>—Line error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PCV</strong>—Pulse code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEFS-S</strong>—Severely errored framing seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES</strong>—Severely errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS</strong>—Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>YELLOW</strong>—Errors at the remote site receiver</td>
<td></td>
</tr>
<tr>
<td><strong>Interface transmit queues</strong></td>
<td>Names of the transmit queues and their associated statistics for each E1 channel on the Channelized STM1-to-E1 PIC.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>B/W</strong>—Queue bandwidth as a percentage of the total interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>WRR</strong>—Weighted round-robin (in percent).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—Number of bytes transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Number of packet errors.</td>
<td></td>
</tr>
<tr>
<td><strong>HDLC configuration</strong></td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Giant threshold</strong>—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt threshold</strong>—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Timeslots</strong>—Configured time slots for the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Line encoding</strong>—Line encoding used. It is always HDB3.</td>
<td></td>
</tr>
</tbody>
</table>
Table 37: Channelized STM1 show 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><strong>DS1 BERT configuration</strong></td>
<td>BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• BERT time period</td>
<td>Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td>• Elapsed</td>
<td>Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td>• Induced error rate</td>
<td>Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td>• Algorithm</td>
<td>Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
<tr>
<td><strong>SDH PHY</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td>• Seconds</td>
<td>Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td>• Count</td>
<td>Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td>• State</td>
<td>State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• PLL Lock</td>
<td>Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td>• PHY Light</td>
<td>Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td><strong>SDH regenerator section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td>• Seconds</td>
<td>Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td>• Count</td>
<td>Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td>• State</td>
<td>State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RS-BIP8</td>
<td>24-bit BIP for multiplex section overhead (B2 bytes)</td>
<td></td>
</tr>
<tr>
<td>• OOF</td>
<td>Out of frame</td>
<td></td>
</tr>
<tr>
<td>• LOS</td>
<td>Loss of signal</td>
<td></td>
</tr>
<tr>
<td>• LOF</td>
<td>Loss of frame</td>
<td></td>
</tr>
<tr>
<td>• RS-ES</td>
<td>Errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td>• RS-SES</td>
<td>Severely errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td>• RS-SEFS</td>
<td>Severely errored framing seconds (regenerator section)</td>
<td></td>
</tr>
</tbody>
</table>
Table 37: Channelized STM1 show 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><strong>SDH multiplex section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-BIP24</strong>—8-bit BIP for high-order path overhead (B3 byte)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-FEBE</strong>—Far-end block error (multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-FERF</strong>—Far-end remote fail (multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-AIS</strong>—alarm indication signal (multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-ES</strong>—Errored seconds (near-end multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-SES</strong>—Severely errored seconds (near-end multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-UAS</strong>—Unavailable seconds (near-end multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-ES-FE</strong>—Errored seconds (far-end multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-SES-FE</strong>—Severely errored seconds (far-end multiplex section)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MS-UAS-FE</strong>—Unavailable seconds (far-end multiplex section)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SDH path</strong></th>
<th>Active alarms and defects, plus counts of specific SDH errors with detailed information.</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-BIP8</strong>—8-bit BIP for regenerator section overhead (B1 byte)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-FEBE</strong>—Far-end block error (high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-LOP</strong>—Loss of pointer (high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-AIS</strong>—High-order-path alarm indication signal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-FERF</strong>—Far-end remote fail (high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-UNEQ</strong>—Unequipped (high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-PLM</strong>—Payload label mismatch (high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-ES</strong>—Errored seconds (near-end high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-SES</strong>—Severely errored seconds (near-end high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-UAS</strong>—Unavailable seconds (near-end high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-ES-FE</strong>—Errored seconds (far-end high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-SES-FE</strong>—Severely errored seconds (far-end high-order path)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>HP-UAS-FE</strong>—Unavailable seconds (far-end high-order path)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 37: Channelized STMI show 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><strong>SDH tu</strong></td>
<td>Active alarms and defects, plus counts of specific SDH tributary unit (TU) errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td>• Seconds</td>
<td>Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td>• Count</td>
<td>Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td>• State</td>
<td>State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td>Subfields are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• TU-BIP-2</td>
<td>Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td>• TU-FEBE</td>
<td>(near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-LOP</td>
<td>Loss of pointer (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-AIS</td>
<td>Alarm indication signal (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-FERF</td>
<td>(near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-UNEQ</td>
<td>Unequipped (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-PLM</td>
<td>Payload label mismatch (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-ES</td>
<td>Errored seconds (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-SES</td>
<td>Severely errored seconds (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-UAS</td>
<td>Unavailable seconds (near-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-ES-FE</td>
<td>Errored seconds (far-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-SES-FE</td>
<td>Severely errored seconds (far-end TU)</td>
<td></td>
</tr>
<tr>
<td>• TU-UAS-FE</td>
<td>Unavailable seconds (far-end TU)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Received SDH overhead</th>
<th>Transmitted SDH overhead</th>
<th>Values of the received and transmitted SONET overhead:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• C2</td>
<td>Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FI</td>
<td>Section user channel byte. This byte is set aside for the purposes of users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• K1 and K2</td>
<td>These bytes are allocated for APS signaling for the protection of the multiplex section.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• J0</td>
<td>Section trace. This byte is defined for STS-1 number 1 of an STS-N signal. Used to transmit a 1-byte fixed-length string or a 16-byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• S1</td>
<td>Synchronization status. The S1 byte is located in the first STS-1 of an STS-N signal.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Z3 and Z4</td>
<td>Allocated for future use.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Received path trace | Transmitted path trace | Channelized OCl2 interfaces allow path trace bytes to be sent inband across the SONET/SDH link. The received path trace value is the message received from the router at the other end of the fiber. The transmitted path trace value is the message that this router transmits. This information is specific to each of the 12 channelized OCl2 interfaces. | extensive |

<table>
<thead>
<tr>
<th>Packet Forwarding Engine configuration</th>
<th>Information about the configuration of the Packet Forwarding Engine:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Destination slot</td>
<td>FPC slot number.</td>
<td></td>
</tr>
<tr>
<td>• PLP byte</td>
<td>Packet Level Protocol byte.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 37: Channelized STM1 show 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><strong>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>• CoS transmit queue</td>
<td>Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth %</td>
<td>Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth bps</td>
<td>Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td>• Buffer %</td>
<td>Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Buffer usec</td>
<td>Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td>• Priority</td>
<td>Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td>• Limit</td>
<td>Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

### Logical Interface

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td></td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, or mpls.</td>
<td></td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td></td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
</tbody>
</table>
Table 37: Channelized STM1 show 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>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following: • Active—Set when the link is active and the DTE and DCE are exchanging information. • Down—Set when the link is active, but no information is received from the DCE. • Unconfigured—Set when the corresponding DLCI in the DCE is not configured. • Configured—Set when the corresponding DLCI in the DCE is configured. • Dce-configured—Displayed when the command is issued from the DTE.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active DLCI—Number of active DLCIs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inactive DLCI—Number of inactive DLCIs.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show interfaces extensive (Channelized STM1, SDH)

user@host> show interfaces e1-1/0/0:1 extensive

Physical interface: e1-1/0/0:1, Enabled, Physical link is Up
Interface index: 148, SNMP ifIndex: 285, Generation: 2915
Link-level type: Frame-relay, MTU: 1504, SDH mode, Speed: E1, Loopback: None, FCS: 16, Framing: G704
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
DTE statistics:
Enquiries sent : 43186
Full enquiries sent : 8515
Enquiry responses received : 43185
Full enquiry responses received : 8515
DCE statistics:
Enquiries received : 0
Full enquiries received : 0
Enquiry responses sent : 0
Full enquiry responses sent : 0
Common statistics:
Unknown messages received : 0
Asynchronous updates received : 0
Out-of-sequence packets received : 0

Chapter 14: Interface Operational Commands
Keepalive responses timed out       : 0
Nonmatching DCE-end DLCIs:
  2
Hold-times     : Up 0 ms, Down 0 ms
Last flapped   : 2002-05-23 17:02:59 PDT (17:23:45 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes :                  592                   48 bps
  Output bytes :                  644                   48 bps
  Input packets:                   46                    0 pps
  Output packets:                   46                    0 pps
Input errors:
  Errors: 0, Drops: 9, Framing errors: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 11, L2 mismatch timeouts: 0,
  HS link CRC errors: 0, SRAM errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0
DS1   alarms : None
DS1   defects : None
SDH   alarms : None
SDH   defects : None
E1  media:

<table>
<thead>
<tr>
<th>E1 media</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEF</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BEE</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>AIS</td>
<td>124</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>124</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>YELLOW</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BPV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EXZ</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LCV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PCV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CS</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>FEBE</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LES</td>
<td>124</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>ES</td>
<td>125</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES</td>
<td>124</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEFS</td>
<td>124</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BES</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>UAS</td>
<td>37</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interface transmit queues:

<table>
<thead>
<tr>
<th>Queue</th>
<th>B/W</th>
<th>WR</th>
<th>Packets</th>
<th>Bytes</th>
<th>Drops</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue0</td>
<td>95</td>
<td>95</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Queue1</td>
<td>5</td>
<td>5</td>
<td>529</td>
<td>6348</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

HDLC configuration:
  Giant threshold: 0, Runt threshold: 0
  Timeslots : All active
  Line encoding: HDB3

DS1 BERT configuration:
  BERT time period: 10 seconds, Elapsed: 0 seconds
  Induced Error rate: 10e-0, Algorithm: 2\times15 - 1, 0.151, Pseudorandom (9)

SDH PHY:

<table>
<thead>
<tr>
<th>SDH PHY</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL Lock</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>PHY Light</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

SDH regenerator section:

<table>
<thead>
<tr>
<th>SDH regenerator</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-BIP8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>OOF</td>
<td>125</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>125</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>125</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>RS-ES</td>
<td>125</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RS-SES                  125
RS-SEFS                 125
SDH multiplex section:
    MS-BIP24                  0            0
    MS-FEBE                   0            0
    MS-FERF                   0            0  OK
    MS-AIS                  125            1  OK
    BERR-SF                   0            0
    BERR-SD                   0            0
    MS-ES                  125
    MS-SES                  125
    MS-UAS                  115
    MS-ES-FE                 0
    MS-SES-FE                 0
    MS-UAS-FE                 0
SDH path:
    HP-BIP8                  0            0
    HP-FEBE                   0            0
    HP-LOP                   0            0  OK
    HP-AIS                  125            1  OK
    HP-FERF                   0            0  OK
    HP-UNEQ                   0            0
    HP-PLM                  125            1  OK
    HP-ES                  125
    HP-SES                  125
    HP-UAS                  115
    HP-ES-FE                 0
    HP-SES-FE                 0
    HP-UAS-FE                 0
SDH tu:
    TU-BIP2                  0            0
    TU-FEBE                 124            1
    TU-LOP                   0            0  OK
    TU-AIS                 124            1  OK
    TU-FERF                 124            1  OK
    TU-UNEQ                   0            0
    TU-PLM                 124            1  OK
    TU-ES                  125
    TU-SES                  125
    TU-UAS                  115
    TU-ES-FE                 0
    TU-SES-FE                 0
    TU-UAS-FE                 0
Received SDH overhead:
    F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0x02, Z3      : 0x00, Z4      : 0x00
    V5(cmp) : 0x00
Transmitted SDH overhead:
    F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0x02, Z3      : 0x00, Z4      : 0x00
    V5(cmp) : 0x00
Received path trace:
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Transmitted path trace:
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Packet Forwarding Engine configuration:
    Destination slot: 1, PLP byte: 2 (0x07)
CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Usage</td>
<td>bps</td>
<td>%</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>1945600</td>
<td>95</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>102400</td>
<td>5</td>
</tr>
</tbody>
</table>

Logical interface e1-1/0/1.0 (Index 10) (SNMP ifIndex 369) (Generation 496)
Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 1500, Generation: 575, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255,
  Generation: 975
DLCI 100
  Flags: Active, Dce-configured
  Total down time: 0 sec, Last down: Never
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0

DLCI statistics:
  Active DLCI :2 Inactive DLCI : 0
show interfaces (Channelized T1 IQ)

Syntax

```
show interfaces (ct1-fpc/pic/port | type-fpc/pic/port:<channel>:<channel>)
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced in Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized T1 IQ interface.

Options

- **type-fpc/pic/port:channel**—Interface type. With optional corresponding channel levels, the interface type can be one of the following:
  - **type-fpc/pic/port**—For the physical channelized T1 IQ interface, **type** is ct1.
  - **type-fpc/pic/port:channel**—For the clear channel, **type** is t1. At the first level of channelization, **type** can be ct1 or t1.
  - **type-fpc/pic/port:channel:channel**—At the second level of channelization, **type** can be ds.

- **brief | detail | extensive | terse**—(Optional) Display the specified level of output.
- **descriptions**—(Optional) Display interface description strings.
- **media**—(Optional) Display media-specific information about network interfaces.
- **snmp-index snmp-index**—(Optional) Display information for the specified SNMP index of the interface.
- **statistics**—(Optional) Display static interface statistics.

Required Privilege

**view**

List of Sample Output

- show interfaces extensive (CT1) on page 1363
- show interfaces extensive (T1) on page 1364
- show interfaces extensive (DS0) on page 1365

Output Fields

Table 38 on page 1356 lists the output fields for the `show interfaces` (Channelized T1 IQ and T3 IQ interfaces) command. Output fields are listed in the approximate order in which they appear.
### Table 38: Channelized T1 IQ and T3 IQ show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field”</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface’s index number, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>Physical layer framing format used on the link. It can be ESF or SF. The default is</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>ESF.</td>
<td></td>
</tr>
<tr>
<td>Parent</td>
<td>Name and interface index of the interface to which a particular child interface</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>belongs. None indicates that this interface is the top level.</td>
<td></td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>“Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags”</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 38: Channelized T1 IQ and T3 IQ show 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>Keepalive settings</td>
<td>Configured settings for keepalives.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>interval seconds</td>
<td>— The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.</td>
<td></td>
</tr>
<tr>
<td>down-count number</td>
<td>— The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.</td>
<td></td>
</tr>
<tr>
<td>up-count number</td>
<td>— The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.</td>
<td></td>
</tr>
<tr>
<td>Keepalive statistics</td>
<td>Information about keepalive packets.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input</td>
<td>— Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td>(last seen 00:00:00 ago)</td>
<td>— Time since the last keepalive packet was received, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>— Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td>(last seen 00:00:00 ago)</td>
<td>— Time since the last keepalive packet was sent, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td>LMI settings</td>
<td>(Frame Relay) Settings for Local Management Interface (LMI) can be either ANSI LMI settings or ITU LMI settings. ANSI LMI settings is the default. The format is (ANSI or ITU) LMI settings: value, value..., xx seconds, where value can be:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>n391dte</td>
<td>— DTE full status polling interval (1–255)</td>
<td></td>
</tr>
<tr>
<td>n392dce</td>
<td>— DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td>n392dte</td>
<td>— DTE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td>n393dce</td>
<td>— DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td>n393dte</td>
<td>— DTE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td>t391dte</td>
<td>— DTE polling timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td>t392dce</td>
<td>— DCE polling verification timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td>LMI</td>
<td>(Frame Relay) LMI packet statistics:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input</td>
<td>— Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input:nn (last seen hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td>Output</td>
<td>— Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output:nn (last sent hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td>DTE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data communication equipment (DCE):</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Enquiries sent</td>
<td>— Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>Full enquiries sent</td>
<td>— Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>Enquiry responses received</td>
<td>— Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td>Full enquiry responses received</td>
<td>— Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 38: Channelized T1 IQ and T3 IQ show 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><strong>DCE statistics</strong></td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enquiries received</strong> — Number of enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Full enquiries received</strong> — Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Enquiry responses sent</strong> — Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Full enquiry responses sent</strong> — Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown messages received</strong> — Number of received packets that do not fall into any category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Asynchronous updates received</strong> — Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Out-of-sequence packets received</strong> — Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Keepalive responses timed out</strong> — Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay) Number of DLCIs configured from the DCE, displayed only from the DTE.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-received</strong> — Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-sent</strong> — Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-req-sent</strong> — Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong> — LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not-configured</strong> — LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong> — LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-received</strong> — Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-sent</strong> — Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-req-sent</strong> — Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong> — NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not-configured</strong> — NCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong> — NCP negotiation is successful.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 38: Channelized T1 IQ and T3 IQ show 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><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-received</strong>—Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-sent</strong>—Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-received</strong>—Response was received for the challenge sent, but CHAP has not yet moved into the <strong>Success</strong> state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-sent</strong>—Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failure</strong>—CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong>—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is <strong>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</strong>. For example, <strong>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</strong>.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes, Output bytes</strong>—Number of bytes received and transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets, Output packets</strong>—Number of packets received and transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 38: Channelized T1 IQ and T3 IQ show 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><strong>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Counter increments when the software could not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Count of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Count of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SRAM errors</strong>—Number of hardware errors that occurred in the static RAM (SRAM) on the PIC. If the value in this field increments, the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeds the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 38: Channelized T1 IQ and T3 IQ show 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><strong>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>DS1 alarms DS1 defects</strong></td>
<td>Media-specific defects that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface.</td>
<td><strong>detail extensive none</strong></td>
</tr>
<tr>
<td></td>
<td>• LOS—Loss of signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOF—Loss of frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS—Alarm indication signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• YLW—Yellow alarm. Indicates errors at the remote site receiver.</td>
<td></td>
</tr>
<tr>
<td><strong>T1 media</strong></td>
<td>Counts of T1 media-specific errors.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The T1 media-specific error types can be:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS—Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BEE—Bit error event</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BES—Bit error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BPV—Bipolar violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CS—Carrier state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ES—Errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EXZ—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FEBE—Far-end block error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LCV—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LES—Line error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOF—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOS—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PCV—Pulse code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SEF—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SEFS—Severely errored framing seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SES—Severely errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UAS—Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• YELLOW—Errors at the remote site receiver</td>
<td></td>
</tr>
<tr>
<td><strong>Line encoding</strong></td>
<td>Line encoding used: <strong>B8ZS</strong> or <strong>AMI</strong>.</td>
<td><strong>All levels</strong></td>
</tr>
<tr>
<td><strong>Buildout</strong></td>
<td>Buildout setting.</td>
<td><strong>All levels</strong></td>
</tr>
</tbody>
</table>
**Table 38: Channelized T1 IQ and T3 IQ show 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><strong>HDLC configuration</strong></td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td>• Policing bucket</td>
<td>Configured state of the receiving policer.</td>
<td></td>
</tr>
<tr>
<td>• Shaping bucket</td>
<td>Configured state of the transmitting shaper.</td>
<td></td>
</tr>
<tr>
<td>• Giant threshold</td>
<td>Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td>• Runt threshold</td>
<td>Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td>• Timeslots</td>
<td>Configured time slots for the interface.</td>
<td></td>
</tr>
<tr>
<td>• Line encoding</td>
<td>Line encoding used: B8ZS or AMI.</td>
<td></td>
</tr>
<tr>
<td>• Byte encoding</td>
<td>Byte encoding used: Nx64K or Nx56K.</td>
<td></td>
</tr>
<tr>
<td>• Data inversion</td>
<td>HDLC data inversion setting: Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td>• Idle cycle Flag</td>
<td>Idle cycle flags.</td>
<td></td>
</tr>
<tr>
<td>• Start end Flag</td>
<td>Start and end flag.</td>
<td></td>
</tr>
<tr>
<td><strong>DS0 or DS1 BERT configuration</strong></td>
<td>BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• BERT time period</td>
<td>Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td>• Elapsed</td>
<td>Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td>• Induced error rate</td>
<td>Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td>• Algorithm</td>
<td>Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
<tr>
<td><strong>Packet Forwarding Engine configuration</strong></td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Destination slot</td>
<td>FPC slot number.</td>
<td></td>
</tr>
<tr>
<td>• PLP byte</td>
<td>Packet Level Protocol byte.</td>
<td></td>
</tr>
<tr>
<td><strong>Logical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface; values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, or mpls.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 38: Channelized T1 IQ and T3 IQ show 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>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active—Set when the link is active and the DTE and DCE are exchanging information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Set when the link is active, but no information is received from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unconfigured—Set when the corresponding DLCI in the DCE is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured—Set when the corresponding DLCI in the DCE is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dce-configured—Displayed when the command is issued from the DTE.</td>
<td></td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active DLCI—Number of active DLCIs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inactive DLCI—Number of inactive DLCIs.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show interfaces extensive (CTI)

```
user@host> show interfaces extensive ct1-0/1/1

Physical interface: ct1-0/1/1, Enabled, Physical link is Up
  Interface index: 145, SNMP ifIndex: 32, Generation: 28
  Link-level type: Controller, Clocking: Internal, Speed: T1,
  Loopback: None, Framing: ESF, Parent: None
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps 16384
  Link flags : None
  Hold-times : Up 0 ms, Down 0 ms
  CoS queues : 4 supported
```
show interfaces extensive (T1)

user@host> show interfaces extensive t1-0/2/0

Physical interface: t1-0/2/0, Enabled, Physical link is Up
  Interface index: 161, SNMP ifIndex: 33, Generation: 61
  Link-level type: PPP, MTU: 1504, Speed: T1, Loopback: None, FCS: 16,
  Parent: ct1-0/2/0 Interface index 148
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps 16384
  Link flags : Keepalives DTE
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)

DTE statistics:
  Enquiries sent : 43186
  Full enquiries sent : 8515
  Enquiry responses received : 43185
  Full enquiry responses received : 8515

DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0

Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0

Nonmatching DCE-end DLCIs:
  2
show interfaces extensive (DS0)

user@host> show interfaces extensive ds-0/1/0:0

Physical interface: ds-0/1/0:1, Enabled, Physical link is Up
    Interface index: 157, SNMP ifIndex: 52, Generation: 46
    Link-level type: Frame-Relay, PPP, MTU: 1504, Clocking: Internal,
    Speed: 640kbps, Loopback: None, FCS:16,
    Parent: ct1-0/1/0 Interface index 143
Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps 16384
    Link flags : Keepalives DTE
    ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
    LMI: Input: 51700 (00:00:02 ago), Output: 51701 (00:00:02 ago)
DTE statistics:
    Enquiries sent : 43186
    Full enquiries sent : 8515
    Enquiry responses received : 43185
    Full enquiry responses received : 8515
DCE statistics:
    Enquiries received : 0
    Full enquiries received : 0
    Enquiry responses sent : 0
    Full enquiry responses sent : 0
Common statistics:
    Unknown messages received : 0
Asynchronous updates received : 0
Out-of-sequence packets received : 0
Keepalive responses timedout : 0

Nonmatching DCE-end DLCIs:

2

Hold-times : Up 0 ms, Down 0 ms

Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3

Keepalive statistics:
Input : 8 (last seen 00:00:12 ago)
Output: 8 (last sent 00:00:07 ago)

LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured

CHAP state: Not-configured

CoS queues : 4 supported

Last flapped : 2005-08-18 15:23:46 PDT (00:03:17 ago)
Statistics last cleared: 2005-08-18 15:25:37 PDT (00:01:26 ago)

Traffic statistics:
Input bytes : 840 0 bps
Output bytes : 912 0 bps
Input packets: 25 0 pps
Output packets: 26 0 pps

Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, L3 incompletes: 0,
L2 channel errors: 0, L2 mismatch timeouts: 0, HS link CRC errors: 0,
Resource errors: 0

Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0,
MTU errors: 0, Resource errors: 0

Queue counters:
0 best-effort: Queued packets Transmitted packets Dropped packets
0 expedited-fo
1 assured-forw
2 network-cont
3 network-cont

HDLC configuration:
Giant threshold: 1514, Runt threshold: 2
Timeslots: 1-10
Byte encoding: Nx64K, Data inversion: Disabled, Idle cycle flag: flags,
Start end flag: shared

DSO BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)

Packet Forwarding Engine configuration:
Destination slot: 0, PLP byte: 4 (0x00)

Logical interface ds-0/1/0:1.0 (Index 67) (SNMP ifIndex 53) (Generation 11)
Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 1500, Generation: 26, Route table: 0

Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 11.11.11.0/30, Local: 11.11.11.2, Broadcast: 11.11.11.3,
Generation: 39

DLCI 100
Flags: Active, Dce-configured
Total down time: 0 sec, Last down: Never
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
<table>
<thead>
<tr>
<th>DLCI statistics:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active DLCI : 2 Inactive DLCI : 0</td>
</tr>
</tbody>
</table>

...
show interfaces (Channelized T3 IQ)

Syntax

```ini
show interfaces (ct3-fpc/pic/port | type-fpc/pic/port:<channel>:<channel>)
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified channelized T3 IQ interface.

Options

- `type-fpc/pic/port:channel`—Interface type. With optional corresponding channel levels, the interface type can be one of the following:
  - `type-fpc/pic/port`—For the physical channelized T3 IQ interface, `type` is `ct3`.
  - `type-fpc/pic/port:channel`—For the clear channel, `type` is `t3`. At the first level of channelization, `type` can be `ct1` or `t1`.
  - `type-fpc/pic/port:channel:channel`—At the second level of channelization, `type` is `ds`.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

Required Privilege

`view`

List of Sample Output

- `show interfaces extensive (Channelized T3 IQ) (Physical)` on page 1369
- `show interfaces extensive (Channelized T1 on Channelized T3 IQ)` on page 1369
- `show interfaces extensive (DS0 on Channelized T3 IQ)` on page 1369

Output Fields

See the output field table for the `show interfaces (Channelized T1 IQ)` command.
### Sample Output

#### show interfaces extensive (Channelized T3 IQ) (Physical)

```
user@host> show interfaces extensive ct3-0/0/1
Physical interface: ct3-0/0/1, Enabled, Physical link is Up
  Interface index: 30, SNMP ifIndex: 317, Generation: 29
  Link-level type: Controller, MTU: 4474, Clocking: Internal, Speed: T3,
  Loopback: None, FCS: 16, Mode: C/Bit parity, Parent: None
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : None
...
```

#### show interfaces extensive (Channelized T1 on Channelized T3 IQ)

```
user@host> show interfaces extensive ct1-0/0/1:2
Physical interface: ct1-0/0/1:2, Enabled, Physical link is Up
  Interface index: 175, SNMP ifIndex: 1505, Generation: 174
  Link-level type: Controller, MTU: 1504, Clocking: Internal, Speed: T1,
  Loopback: None, FCS: 16, Framing: ESF, Parent: ct3-0/0/1 (Index 32)
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : None
...
```

#### show interfaces extensive (DS0 on Channelized T3 IQ)

```
user@host> show interfaces extensive ds-0/0/1:2:1
Physical interface: ds-0/0/1:2:1, Enabled, Physical link is Up
  Interface index: 176, SNMP ifIndex: 1563, Generation: 175
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: 640kbps,
  Loopback: None, FCS: 16, Parent: ct1-0/0/1:2 (Index 175)
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
...
```
show interfaces (Discard)

Syntax

    show interfaces dsc
    <brief | detail | extensive | terse>
    <descriptions>
    <media>
    <snmp-index snmp-index>
    <statistics>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display status information about the specified discard interface.

Options

dsc—Display standard information about the specified discard interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—This option is not relevant for the discard interface and always shows a value of 0.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) This option is not relevant for the discard interface and always shows a value of 0.

Required Privilege

Level

view

Related Documentation

- show interfaces (ATM) on page 1244
- show interfaces routing

List of Sample Output

- show interfaces dsc on page 1373
- show interfaces dsc brief on page 1373
- show interfaces dsc detail on page 1374
- show interfaces dsc extensive on page 1374

Output Fields

Table 39 on page 1370 lists the output fields for the show interfaces (discard) command. Output fields are listed in the approximate order in which they appear.

Table 39: Discard show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></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>Physical interface</td>
<td>Name of the physical interface, whether the interface is enabled, and the state of the physical interface: <strong>Up or Down.</strong></td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface. <strong>Software-Pseudo</strong> indicates a standard software interface with no associated hardware device.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be <strong>Internal</strong> or <strong>External</strong>.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Physical info</td>
<td>Information about the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down. Value is in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address, Hardware address</td>
<td>Configured MAC address and hardware MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup address of the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is <strong>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</strong>. For example, <strong>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</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>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes, Output bytes</strong>—Number of bytes received and transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets, Output packets</strong>—Number of packets received and transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Output errors</td>
<td>(Extensive only) Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Logical interface</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 39: Discard show 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><strong>Flags</strong></td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol family configured on the logical interface, such as iso, inet6, or mpls.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Route Table</strong></td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

### Sample Output

#### show interfaces dsc

```plaintext
user@host> show interfaces dsc
Physical interface: dsc, Enabled, Physical link is Up
    Interface index: 5, SNMP ifIndex: 5
    Type: Software-Pseudo, MTU: Unlimited
    Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps
    Link flags : None
    Last flapped : Never
    Input packets : 0
    Output packets: 0

Logical interface dsc.0 (Index 66) (SNMP ifIndex 235)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Unspecified
    Protocol inet, MTU: Unlimited
    Flags: None
```

#### show interfaces dsc brief

```plaintext
user@host> show interfaces dsc brief
Physical interface: dsc, Enabled, Physical link is Up
    Type: Software-Pseudo, Link-level type: Unspecified, MTU: Unlimited, Clocking: Unspecified, Speed: Unspecified
    Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps

Logical interface dsc.0
    Flags: Point-To-Point SNMP-Traps Encapsulation: Unspecified
    inet
```
show interfaces dsc detail

Physical interface: dsc, Enabled, Physical link is Up
  Interface index: 5, SNMP ifIndex: 5, Generation: 9
  Type: Software-Pseudo, Link-level type: Unspecified, MTU: Unlimited, Clocking: Unspecified, Speed: Unspecified
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type : Unspecified
  Link flags : None
  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 : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0

Logical interface dsc.0 (Index 66) (SNMP ifIndex 235) (Generation 6)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Unspecified
  Protocol inet, MTU: Unlimited, Generation: 14, Route table: 0
  Flags: None

show interfaces dsc extensive

Physical interface: dsc, Enabled, Physical link is Up
  Interface index: 5, SNMP ifIndex: 5, Generation: 9
  Type: Software-Pseudo, Link-level type: Unspecified, MTU: Unlimited, Clocking: Unspecified, Speed: Unspecified
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type : Unspecified
  Link flags : None
  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 : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
    Input errors:
      Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
      Policed discards: 0, Resource errors: 0
    Output errors:
      Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
      Resource errors: 0

Logical interface dsc.0 (Index 66) (SNMP ifIndex 235) (Generation 6)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Unspecified
Protocol inet, MTU: Unlimited, Generation: 14, Route table: 0
show interfaces (Fast Ethernet)

Syntax

```
show interfaces interface-type
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display status information about the specified Fast Ethernet interface.

Options

- `interface-type`—On M Series and T Series routers, the interface type is `fe-fpc/pic/port`.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

Required Privilege Level

`view`

List of Sample Output

- `show interfaces (Fast Ethernet)` on page 1390
- `show interfaces brief (Fast Ethernet)` on page 1390
- `show interfaces detail (Fast Ethernet)` on page 1390
- `show interfaces extensive (Fast Ethernet)` on page 1391

Output Fields

Table 40 on page 1376 lists the output fields for the `show interfaces (Fast Ethernet)` 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>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-mode</td>
<td>Type of link connection configured for the physical interface: Full-duplex or Half-duplex</td>
<td>extensive</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: Enabled or Disabled. If loopback is enabled, type of loopback: Local or Remote.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>LAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.</td>
<td>All levels</td>
</tr>
<tr>
<td>WAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>Unidirectional link mode status for 10-Gigabit Ethernet interface: Enabled or Disabled for parent interface; Rx-only or Tx-only for child interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Remote-fault</td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Online—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offline—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Wavelength</td>
<td>(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
### Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).</td>
<td>All levels</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Schedulers</td>
<td>(GigabitEthernet intelligent queuing 2 (IQ2) interfaces only) Number of CoS schedulers configured.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet and 10-Gigabit Ethernet IQ PICs count the overhead and CRC bytes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Gigabit Ethernet IQ PICs, the input byte counts vary by interface type. For more information, see Table 31 under the show interfaces command.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 40: show interfaces Fast Ethernet 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>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <code>ignore-l3-incompletes</code> statement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Collisions</strong>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Egress queues</td>
<td>Total number of egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> In DPCs that are not of the enhanced type, such as DPC 40x1GE R, DPCE 20x1GE + 2x10GE R, or DPCE 40x1GE R, you might notice a discrepancy in the output of the <strong>show interfaces</strong> command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs.</td>
<td></td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>(Egress)</td>
<td>• <strong>Queued packets</strong>—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dropped packets</strong>—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
</tbody>
</table>
Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress queues</td>
<td>Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td>(Ingress)</td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Active alarms and Active defects</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the routing device configuration, an alarm can ring the red or yellow alarm bell on the routing device, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>OTN FEC statistics</td>
<td>The forward error correction (FEC) counters provide the following statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corrected Errors—The count of corrected errors in the last second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corrected Error Ratio—The corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits.</td>
<td></td>
</tr>
<tr>
<td>PCS statistics</td>
<td>(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Bit errors—The number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errored blocks—The number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC statistics</td>
<td><strong>Receive and Transmit</strong> statistics reported by the PIC's MAC subsystem, including the following:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total octets and total packets</strong>—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. For more information, see Table 31 under the <code>show interfaces</code> command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unicast packets, Broadcast packets, and Multicast packets</strong>—Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC/Align errors</strong>—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO error</strong>—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC control frames</strong>—Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC pause frames</strong>—Number of MAC control frames with pause operational code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Oversized frames</strong>—Number of frames that exceed 1518 octets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Jabber frames</strong>—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fragment frames</strong>—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN tagged frames</strong>—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Code violations</strong>—Number of times an event caused the PHY to indicate “Data reception error” or “Invalid data symbol error”</td>
<td></td>
</tr>
</tbody>
</table>

| OTN Received Overhead Bytes | APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08 | extensive       |

| OTN Transmitted Overhead Bytes | APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08 | extensive       |
Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter statistics</td>
<td>Receive and Transmit statistics reported by the PIC's MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet's source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>* Input packet count—Number of packets received from the MAC hardware that the filter processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Input packet rejects—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Input DA rejects—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the routing device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local routing device (which the routing device is rejecting).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Input SA rejects—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Output packet count—Number of packets that the filter has given to the MAC hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Output packet pad count—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* Output packet error count—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* CAM destination filters, CAM source filters—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0.</td>
<td></td>
</tr>
</tbody>
</table>

**PMA PHY** (10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:                                                                                                                                                                                                                                                      | extensive       |
|                    | * Seconds—Number of seconds the defect has been active.                                                                                                                                                                                                                                                                                        |                 |
|                    | * Count—Number of times that the defect has gone from inactive to active.                                                                                                                                                                                                        |                 |
|                    | * State—State of the error. Any state other than OK indicates a problem.                                                                                                                                                                                                       |                 |

Subfields are:

- **PHY Lock**—Phase-locked loop
- **PHY Light**—Loss of optical signal
### Table 40: `show interfaces Fast Ethernet Output Fields (continued)`

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| **WIS section** | (10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:  
- **Seconds**—Number of seconds the defect has been active.  
- **Count**—Number of times that the defect has gone from inactive to active.  
- **State**—State of the error. Any state other than **OK** indicates a problem.  
Subfields are:  
- **BIP-B1**—Bit interleaved parity for SONET section overhead  
- **SEF**—Severely errored framing  
- **LOL**—Loss of light  
- **LOF**—Loss of frame  
- **ES-S**—Errored seconds (section)  
- **SEFS-S**—Severely errored framing seconds (section) | extensive         |
| **WIS line**  | (10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.  
- **Seconds**—Number of seconds the defect has been active.  
- **Count**—Number of times that the defect has gone from inactive to active.  
- **State**—State of the error. State other than **OK** indicates a problem.  
Subfields are:  
- **BIP-B2**—Bit interleaved parity for SONET line overhead  
- **REI-L**—Remote error indication (near-end line)  
- **RDI-L**—Remote defect indication (near-end line)  
- **AIS-L**—Alarm indication signal (near-end line)  
- **BERR-SF**—Bit error rate fault (signal failure)  
- **BERR-SD**—Bit error rate defect (signal degradation)  
- **ES-L**—Errored seconds (near-end line)  
- **SES-L**—Severely errored seconds (near-end line)  
- **UAS-L**—Unavailable seconds (near-end line)  
- **ES-LFE**—Errored seconds (far-end line)  
- **SES-LFE**—Severely errored seconds (far-end line)  
- **UAS-LFE**—Unavailable seconds (far-end line) | extensive         |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIS path</td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of the error. Any state other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BIP-B3—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REI-P—Remote error indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LOP-P—Loss of pointer (path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AIS-P—Path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RDI-P—Path remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UNEQ-P—Path unequipped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PLM-P—Path payload (signal) label mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ES-P—Errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SES-P—Severely errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UAS-P—Unavailable seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SES-PFE—Severely errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UAS-PFE—Unavailable seconds (far-end STS path)</td>
<td></td>
</tr>
</tbody>
</table>
Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation information</td>
<td>Information about link autonegotiation.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Negotiation status:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Incomplete—Ethernet interface has the speed or link mode configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No autonegotiation—Remote Ethernet interface has the speed or link mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured, or does not perform autonegotiation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Complete—Ethernet interface is connected to a device that performs autonego-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link partner status—OK when Ethernet interface is connected to a device that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link partner:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link mode—Depending on the capability of the attached Ethernet device, either</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full-duplex or Half-duplex.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flow control—Types of flow control supported by the remote Ethernet device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Fast Ethernet interfaces, the type is None. For Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interfaces, types are Symmetric (link partner supports PAUSE on receive and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmit), Asymmetric (link partner supports PAUSE on transmit), and Symmet-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ric/Asymmetric (link partner supports both PAUSE on receive and trans-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mit transmit or only PAUSE receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote fault—Remote fault information from the link partner—Failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates a receive link error. OK indicates that the link partner is receiv-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ing. Negotiation error indicates a negotiation error. Offline indicates that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the link partner is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Local resolution—Information from the link partner:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flow control—Types of flow control supported by the remote Ethernet device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Gigabit Ethernet interfaces, types are Symmetric (link partner supports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAUSE on receive and transmit), Asymmetric (link partner supports PAUSE on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmit), and Symmetric/Asymmetric (link partner supports both PAUSE on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receive and transmit or only PAUSE receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote fault—Remote fault information. Link OK (no error detected on receive),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Offline (local interface is offline), and Link Failure (link error detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on receive).</td>
<td></td>
</tr>
</tbody>
</table>

Received path trace, Transmitted path trace (10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other routing device manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.

Packet Forwarding Engine configuration Information about the configuration of the Packet Forwarding Engine:

• Destination slot—FPC slot number.
### Table 40: show interfaces Fast Ethernet 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>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>CoS transmit queue</strong>—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth %</strong>—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth bps</strong>—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer %</strong>—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer usec</strong>—Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Priority</strong>—Queue priority: <strong>low</strong> or <strong>high</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Limit</strong>—Displayed if rate limiting is configured for the queue. Possible values are <strong>none</strong> and <strong>exact</strong>. If <strong>exact</strong> is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If <strong>none</strong> is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

### Logical Interface

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Index</strong></td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifindex</strong></td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 40: show interfaces Fast Ethernet 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>VLAN-Tag</strong></td>
<td>Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.</td>
<td><strong>brief</strong> <strong>detail</strong> <strong>extensive</strong> none</td>
</tr>
<tr>
<td></td>
<td>- <strong>push</strong>—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>pop</strong>—The outer VLAN tag of the incoming frame is removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>swap</strong>—The outer VLAN tag of the incoming frame is overwritten with the user specified VLAN tag information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>push</strong>—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>push-push</strong>—Two VLAN tags are pushed in from the incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>swap-push</strong>—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>swap-swap</strong>—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user specified VLAN tag value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>pop-swap</strong>—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>pop-pop</strong>—Both the outer and inner VLAN tags of the incoming frame are removed.</td>
<td></td>
</tr>
<tr>
<td><strong>Demux:</strong></td>
<td>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</td>
<td><strong>detail</strong> <strong>extensive</strong> none</td>
</tr>
<tr>
<td></td>
<td>- Source Family Inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Destination Family Inet</td>
<td></td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Encapsulation on the logical interface.</td>
<td><strong>All levels</strong></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol family. Possible values are described in the “Protocol Field” section under “Common Output Fields Description” on page 1152.</td>
<td><strong>detail</strong> <strong>extensive</strong> none</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Maximum transmission unit size on the logical interface.</td>
<td><strong>detail</strong> <strong>extensive</strong> none</td>
</tr>
<tr>
<td><strong>Maximum labels</strong></td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.</td>
<td><strong>detail</strong> <strong>extensive</strong> none</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the specified interface set.</td>
<td><strong>detail</strong> <strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Input bytes, Output bytes</strong>—Number of bytes received and transmitted on the interface set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>input packets, Output packets</strong>—Number of packets received and transmitted on the interface set.</td>
<td></td>
</tr>
<tr>
<td><strong>IPv6 transit statistics</strong></td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td><strong>Local statistics</strong></td>
<td>Number and rate of bytes and packets destined to the routing device.</td>
<td><strong>extensive</strong></td>
</tr>
</tbody>
</table>
### Table 40: show interfaces Fast Ethernet Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the <strong>Output bytes</strong> and <strong>Output packets</strong> interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.</td>
<td></td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Donor interface</td>
<td>(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Preferred source address</td>
<td>(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mac-Validate Failures</td>
<td>Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about address flag (possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
**Table 40: show interfaces Fast Ethernet Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**Sample Output**

**show interfaces (Fast Ethernet)**

```bash
user@host> show interfaces fe-0/0/0

Physical interface: fe-0/0/0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 22
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues : 4 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:38
  Last flapped : 2006-01-20 14:50:58 PST (2w4d 00:44 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  Active alarms : None
  Active defects : None
  Logical interface fe-0/0/0.0 (Index 66) (SNMP ifIndex 198)
    Flags: SNMP-Traps Encapsulation: ENET2
    Protocol inet, MTU: 1500
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255
```

**show interfaces brief (Fast Ethernet)**

```bash
user@host> show interfaces fe-0/0/0 brief

Physical interface: fe-0/0/0, Enabled, Physical link is Up
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Logical interface fe-0/0/0.0
    Flags: SNMP-Traps Encapsulation: ENET2
    inet  203.0.113.1/24
```

**show interfaces detail (Fast Ethernet)**

```bash
user@host> show interfaces fe-0/0/0 detail

Physical interface: fe-0/0/0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 22, Generation: 5391
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues : 4 supported, 4 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:3f:38
```
show interfaces extensive (Fast Ethernet)

user@host> show interfaces fe-0/0/0 extensive

Physical interface: fe-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 22, Generation: 5391
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues : 4 supported, 4 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:38
Last flapped : 2006-01-20 14:50:58 PST (2w4d 00:46 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 42 0 bps
Input packets: 0 0 pps
Output packets: 1 0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Active alarms : None
Active defects : None
MAC statistics:
<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>64</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Interfaces Fundamentals for Routing Devices

Jabber frames 0
Fragment frames 0
VLAN tagged frames 0
Code violations 0

Filter statistics:
  Input packet count 0
  Input packet rejects 0
  Input DA rejects 0
  Input SA rejects 0
  Output packet count 1
  Output packet pad count 0
  Output packet error count 0
  CAM destination filters: 1, CAM source filters: 0

Autonegotiation information:
  Negotiation status: Complete
  Link partner:
    Link partner: Full-duplex, Flow control: None, Remote fault: Ok

Local resolution:
Packet Forwarding Engine configuration:
  Destination slot: 0
CoS information:

| CoS | Bandwidth % | Buffer Priority % | Limit usec | Limit
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>95</td>
<td>950000000</td>
<td>95</td>
<td>low</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>50000000</td>
<td>5</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface fe-0/0/0 (Index 66) (SNMP ifIndex 198) (Generation 67)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500, Generation: 105, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255,
    Generation: 136
**show interfaces**

**List of Syntax**
- Syntax (Gigabit Ethernet) on page 1393
- Syntax (10 Gigabit Ethernet) on page 1393
- Syntax (SRX Series Devices and (vSRX and vSRX 3.0 platforms)) on page 1393

**Syntax (Gigabit Ethernet)**
- `show interfaces ge-fpc/pic/port <brief | detail | extensive | terse>`
- `<descriptions>`
- `<media>`
- `<snmp-index snmp-index>`
- `<statistics>`

**Syntax (10 Gigabit Ethernet)**
- `show interfaces xe-fpc/pic/port <brief | detail | extensive | terse>`
- `<descriptions>`
- `<media>`
- `<snmp-index snmp-index>`
- `<statistics>`

**Syntax (SRX Series Devices and (vSRX and vSRX 3.0 platforms))**
- `show interfaces ( <interface-name> <brief | detail | extensive | terse> <controller interface-name> | <descriptions interface-name> | <destination-class all | destination-class-name logical-interface-name> | <diagnostics optics interface-name> | <far-end-interval interface-fpc/pic/port> | <filters interface-name> | <flow-statistics interface-name> | <interval interface-name> | <load-balancing (detail | interface-name)> | <mac-database mac-address mac-address> | <mc-ae id identifier unit number revertive-info> | <media interface-name> | <policers interface-name> | <queue both-ingress-egress egress forwarding-class forwarding-class ingress l2-statistics> | <redundancy (detail | interface-name)> | <routing brief detail summary interface-name> | <routing-instance (all | instance-name)> | <snmp-index snmp-index> | <source-class all | destination-class-name logical-interface-name> | <statistics interface-name> | <switch-port switch-port number> | <transport pm (all | optics | otn) (all | current | currentday | interval | previousday) (all | interface-name)> | <zone interface-name> )`
**Release Information**

Command introduced before Junos OS Release 7.4 for Gigabit interfaces.
Command introduced in Junos OS Release 8.0 for 10 Gigabit interfaces.
Command modified in Junos OS Release 9.5 for SRX Series devices.
Command introduced in Junos OS Release 18.1 for Gigabit interfaces.
Command modified in Junos OS Release 19.3R1 for MX Series Routers.

Starting in Junos OS Release 19.3R1, Output fields `ifindex` and `speed` is modified in the `show interfaces interface name extensive` command, on all MX Series routers.

- The default behavior of WAN-PHY interface remains the same. The new `precise-bandwidth` option reflects the new speed (9.294Gbps) configured on the supported line cards.
- The WAN-PHY framing mode is supported only on MPC5E and MPC6E line cards.

Command modified in Junos OS Release 19.3R1 for vSRX and vSRX 3.0 platforms to support 1G, 10G, 40G, and 100G Gigabit Ethernet interfaces, for performing CoS operations and to provide better bandwidth for processing traffic during congestion using variant speeds.

**Description**

Display status information about the specified Gigabit Ethernet interface.

(M320, M120, MX Series, and T Series routers only) Display status information about the specified 10-Gigabit Ethernet interface.

Display the IPv6 interface traffic statistics about the specified Gigabit Ethernet interface for MX series routers. The input and output bytes (bps) and packets (pps) rates are not displayed for IFD and local traffic.

Display status information and statistics about interfaces on SRX Series, vSRX, and vSRX 3.0 platforms running Junos OS.

**NOTE:** On SRX Series appliances, on configuring identical IPs on a single interface, you will not see a warning message; instead, you will see a syslog message.

Starting in Junos OS Release 18.4R1, Output fields `Next-hop` and `vpls-status` is displayed in the `show interfaces interface name detail` command, only for Layer 2 protocols on MX480 routers.

**Options**

For Gigabit interfaces:

`ge-fpc/pic/port`—Display standard information about the specified Gigabit Ethernet interface.

Starting in Junos OS Release 19.3R1, on vSRX and vSRX 3.0, this interface can be configured with different speed rates of 1G, 10G, 40G, and 100G. This speed is applied for performing CoS operations and to provide better bandwidth for processing traffic during congestion.
NOTE: Interfaces with different speeds are named uniformly with ge-0/0/x for backward compatibility. Use the show interfaces command to view the interface speeds.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

For 10 Gigabit interfaces:

xe-fpc/pic/port—Display standard information about the specified 10-Gigabit Ethernet interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

For SRX interfaces:

- interface-name—(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number.
  - at-pim/0/port—ATM-over-ADSL or ATM-over-SHDSL interface.
  - ce1-pim/0/port—Channelized E1 interface.
  - cl-0/0/8—3G wireless modem interface for SRX320 devices.
  - ct1-pim/0/port—Channelized T1 interface.
  - dl0—Dialer Interface for initiating ISDN and USB modem connections.
  - e1-pim/0/port—E1 interface.
  - e3-pim/0/port—E3 interface.
  - fe-pim/0/port—Fast Ethernet interface.
  - ge-pim/0/port—Gigabit Ethernet interface.
Starting in Junos OS Release 19.3R1, on vSRX and vSRX 3.0, this interface supports different speed of 1G, 10G, 40G, and 100G. You can configure CoS on these interfaces. This speed is applied for performing CoS operations and to provide better bandwidth for processing traffic during congestion.

- **se-pim/0/port**—Serial interface.
- **t1-pim/0/port**—T1 (also called DS1) interface.
- **t3-pim/0/port**—T3 (also called DS3) interface.
- **wx-slot/0/0**—WAN acceleration interface, for the WXC Integrated Services Module (ISM 200).
- **interface-name**—(Optional) Display standard information about the specified interface. Following is a list of typical interface names. Replace pim with the PIM slot and port with the port number.
  - **at-pim/0/port**—ATM-over-ADSL or ATM-over-SHDSL interface.
  - **cel-pim/0/port**—Channelized E1 interface.
  - **cl-0/0/8**—3G wireless modem interface for SRX320 devices.
  - **ct1-pim/0/port**—Channelized T1 interface.
  - **dl0**—Dialer Interface for initiating ISDN and USB modem connections.
  - **e1-pim/0/port**—E1 interface.
  - **e3-pim/0/port**—E3 interface.
  - **fe-pim/0/port**—Fast Ethernet interface.
  - **ge-pim/0/port**—Gigabit Ethernet interface.

Additional Information

In a logical system, this command displays information only about the logical interfaces and not about the physical interfaces.

Required Privilege

**view**
Starting in Junos OS Release 18.4R1, output fields `Next-hop` and `vpls-status` is displayed in the `show interfaces interface name detail` command, only for Layer 2 protocols on MX480 routers.

### Related Documentation

- Understanding Layer 2 Interfaces on Security Devices
- Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration
- Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers

### List of Sample Output

- `show interfaces (Gigabit Ethernet) on page 1435`
- `show interfaces (Gigabit Ethernet on MX Series Routers) on page 1435`
- `show interfaces (link degrade status) on page 1436`
- `show interfaces extensive (Gigabit Ethernet on MX Series Routers showing interface transmit statistics configuration) on page 1436`
- `show interfaces brief (Gigabit Ethernet) on page 1437`
- `show interfaces detail (Gigabit Ethernet) on page 1437`
- `show interfaces extensive (Gigabit Ethernet IQ2) on page 1439`
- `show interfaces (Gigabit Ethernet Unnumbered Interface) on page 1442`
- `show interfaces (ACI Interface Set Configured) on page 1442`
- `show interfaces (ALI Interface Set) on page 1443`
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, IQ2) on page 1443`
- `show interfaces extensive (10-Gigabit Ethernet, WAN PHY Mode) on page 1445`
- `show interfaces extensive (10-Gigabit Ethernet, DWDM OTN PIC) on page 1447`
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode) on page 1450`
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Transmit-Only) on page 1450`
- `show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Receive-Only) on page 1451`
- Sample Output SRX Gigabit Ethernet on page 1452
- Sample Output SRX Gigabit Ethernet on page 1453
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0) on page 1454`
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0) on page 1454`
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0) on page 1454`
- `show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0) on page 1454`
- `show interfaces detail (Gigabit Ethernet) on page 1455`
- `show interfaces statistics st0.0 detail on page 1456`
- `show interfaces extensive (Gigabit Ethernet) on page 1457`
- `show interfaces terse on page 1460`
- `show interfaces terse (vSRX and vSRX 3.0) on page 1461`
- `show interfaces controller (Channelized E1 IQ with Logical E1) on page 1461`
- `show interfaces controller (Channelized E1 IQ with Logical DS0) on page 1461`
- `show interfaces descriptions on page 1461`
- `show interfaces destination-class all on page 1461`
show interfaces diagnostics optics on page 1462
show interfaces far-end-interval coc12-5/2/0 on page 1463
show interfaces far-end-interval coc1-5/2/1:1 on page 1463
show interfaces filters on page 1463
show interfaces flow-statistics (Gigabit Ethernet) on page 1464
show interfaces interval (Channelized OC12) on page 1465
show interfaces interval (E3) on page 1465
show interfaces interval (SONET/SDH) (SRX devices) on page 1465
show interfaces load-balancing (SRX devices) on page 1466
show interfaces load-balancing detail (SRX devices) on page 1466
show interfaces mac-database (All MAC Addresses on a Port SRX devices) on page 1466
show interfaces mac-database (All MAC Addresses on a Service SRX devices) on page 1467
show interfaces mac-database mac-address on page 1467
show interfaces mc-ae (SRX devices) on page 1468
show interfaces media (SONET/SDH) on page 1468
show interfaces policers (SRX devices) on page 1469
show interfaces policers interface-name (SRX devices) on page 1469
show interfaces queue (SRX devices) on page 1469
show interfaces redundancy (SRX devices) on page 1470
show interfaces redundancy (Aggregated Ethernet SRX devices) on page 1470
show interfaces redundancy detail (SRX devices) on page 1470
show interfaces routing brief (SRX devices) on page 1471
show interfaces routing detail (SRX devices) on page 1471
show interfaces routing-instance all (SRX devices) on page 1472
show interfaces snmp-index (SRX devices) on page 1472
show interfaces source-class all (SRX devices) on page 1472
show interfaces statistics (Fast Ethernet SRX devices) on page 1473
show interfaces switch-port (SRX devices) on page 1473
show interfaces transport pm (SRX devices) on page 1474
show security zones (SRX devices) on page 1475

Output Fields  
Table 30 on page 1166 describes the output fields for the show interfaces (Gigabit Ethernet) command. Output fields are listed in the approximate order in which they appear. For Gigabit Ethernet IQ and IQE PICs, the traffic and MAC statistics vary by interface type. For more information, see Table 31 on page 1195.

Table 41: show interfaces (Gigabit Ethernet) Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical interface</strong></td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface index</strong></td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifindex</strong></td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) 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>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Link-level type</strong></td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Loopback status: Enabled or Disabled. If loopback is enabled, type of loopback:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Local or Remote.</td>
<td></td>
</tr>
<tr>
<td><strong>Source filtering</strong></td>
<td>Source filtering status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>LAN-PHY mode</strong></td>
<td>10-Gigabit Ethernet interface operating in Local Area Network Physical Layer</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>existing Ethernet applications.</td>
<td></td>
</tr>
<tr>
<td><strong>WAN-PHY mode</strong></td>
<td>10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fiber-optic cables and other devices intended for SONET/SDH.</td>
<td></td>
</tr>
<tr>
<td><strong>Unidirectional</strong></td>
<td>Unidirectional link mode status for 10-Gigabit Ethernet interface: Enabled or</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Disabled for parent interface; Rx-only or Tx-only for child interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Flow control</strong></td>
<td>Flow control status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Auto-negotiation</strong></td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: Enabled or Disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Remote-fault</strong></td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Online—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offline—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td><strong>Device flags</strong></td>
<td>Information about the physical device. Possible values are described in the</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>“Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td><strong>Interface flags</strong></td>
<td>Information about the interface. Possible values are described in the “Interface</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Flags” section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td><strong>Link flags</strong></td>
<td>Information about the link. Possible values are described in the “Links Flags”</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>section under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td><strong>Wavelength</strong></td>
<td>(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces)</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Displays the configured wavelength, in nanometers (nm).</td>
<td></td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>with the configured wavelength, in terahertz (THz).</td>
<td></td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></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>Schedulers</td>
<td>(Gigabit Ethernet intelligent queuing 2 [IQ2] interfaces only) Number of CoS schedulers configured.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds (ms).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>none</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps). The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Egress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for egress traffic.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Ingress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for ingress traffic.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface. The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet and 10-Gigabit Ethernet IQ PICs count the overhead and CRC bytes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Gigabit Ethernet IQ PICs, the input byte counts vary by interface type. For more information, see Table 31 under the show interfaces command.</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <code>ignore-l3-incompletes</code> statement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) 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>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Collisions</strong>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number must always be 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field must never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Egress queues</strong></th>
<th>Total number of egress queues supported on the specified interface.</th>
<th>detailed extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE: In DPCs that are not of the enhanced type, such as DPC 40x 1GE R, DPCE 20x 1GE + 2x 10GE R, or DPCE 40x 1GE R, you might notice a discrepancy in the output of the show interfaces command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue counters (Egress)</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Due to accounting space limitations on certain Type 3 FPCs (which are supported in M320 and T640 routers), the Dropped packets field does not always display the correct value for queue 6 or queue 7 for interfaces on 10-port 1-Gigabit Ethernet PICs.</td>
<td></td>
</tr>
<tr>
<td>Ingress queues</td>
<td>Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td>Queue counters (Ingress)</td>
<td>CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Active alarms and Active defects</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value <strong>None</strong> or <strong>Link</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• None—There are no active defects or alarms.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>Interface transmit statistics</td>
<td>(On MX Series devices) Status of the interface-transmit-statistics configuration: Enabled or Disabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Enabled—When the interface-transmit-statistics statement is included in the configuration. If this is configured, the interface statistics show the actual transmitted load on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disabled—When the interface-transmit-statistics statement is not included in the configuration. If this is not configured, the interface statistics show the offered load on the interface.</td>
<td></td>
</tr>
<tr>
<td>OTN FEC statistics</td>
<td>The forward error correction (FEC) counters provide the following statistics:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Corrected Errors—Count of corrected errors in the last second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corrected Error Ratio—Corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 41: show interfaces (Gigabit Ethernet) 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>PCS statistics</strong></td>
<td>(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bit errors</strong>—Number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errored blocks</strong>—Number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Link Degradation</strong></td>
<td>Shows the link degrade status of the physical link and the estimated bit error rates (BERs). This field is available only for the PICs supporting the physical link monitoring feature.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link Monitoring</strong>—Indicates if physical link degrade monitoring is enabled on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Enable</strong>—Indicates that link degrade monitoring has been enabled (using the <code>link-degrade-monitor</code> statement) on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Disable</strong>—Indicates that link degrade monitoring has not been enabled on the interface. If link degrade monitoring has not been enabled, the output does not show any related information, such as BER values and thresholds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link Degradation Set Threshold</strong>—The BER threshold value at which the link is considered degraded and a corrective action is triggered.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link Degradation Clear Threshold</strong>—The BER threshold value at which the degraded link is considered recovered and the corrective action applied to the interface is reverted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Estimated BER</strong>—The estimated bit error rate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link-degrade event</strong>—Shows link degrade event information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Seconds</strong>—Time (in seconds) elapsed after a link degrade event occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Count</strong>—The number of link degrade events recorded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>State</strong>—Shows the link degrade status (example: Defect Active).</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: `show interfaces (Gigabit Ethernet) Output Fields (continued)`

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC statistics</td>
<td><strong>Receive and Transmit</strong> statistics reported by the PIC's MAC subsystem, including the following:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total octets and total packets</strong>—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. For more information, see Table 31 under the <code>show interfaces</code> command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unicast packets, Broadcast packets, and Multicast packets</strong>—Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC/Align errors</strong>—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO error</strong>—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC control frames</strong>—Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC pause frames</strong>—Number of MAC control frames with <strong>pause</strong> operational code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Oversized frames</strong>—There are two possible conditions regarding the number of oversized frames:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet length exceeds interface MTU, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packet length exceeds MRU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Jabber frames</strong>—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fragment frames</strong>—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN tagged frames</strong>—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The 20-port Gigabit Ethernet MIC (MIC-3D-20GE-SFP) does not have hardware counters for VLAN frames. Therefore, the <strong>VLAN tagged frames</strong> field displays 0 when the <code>show interfaces</code> command is executed on a 20-port Gigabit Ethernet MIC. In other words, the number of VLAN tagged frames cannot be determined for the 20-port Gigabit Ethernet MIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Code violations</strong>—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”</td>
<td></td>
</tr>
<tr>
<td>OTN Received Overhead Bytes</td>
<td>APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08</td>
<td>extensive</td>
</tr>
<tr>
<td>OTN Transmitted Overhead Bytes</td>
<td>APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter statistics</td>
<td><strong>Receive</strong> and <strong>Transmit</strong> statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet may enter the system or be rejected.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet count</strong>—Number of packets received from the MAC hardware that the filter processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet rejects</strong>—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input DA rejects</strong>—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the router from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local router (which the router is rejecting).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input SA rejects</strong>—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field must increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet count</strong>—Number of packets that the filter has given to the MAC hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet pad count</strong>—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet error count</strong>—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field must not increment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CAM destination filters, CAM source filters</strong>—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields must be 0.</td>
<td></td>
</tr>
<tr>
<td>PMA PHY</td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PHY Lock</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PHY Light</strong>—Loss of optical signal</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) 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>WIS section</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- State—State of the error. Any state other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- BIP-B1—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SEF—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- LOL—Loss of light</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- LOF—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ES-S—Errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SES-S—Severely errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SEFS-S—Severely errored framing seconds (section)</td>
<td></td>
</tr>
<tr>
<td><strong>WIS line</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects,</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>plus counts of specific SONET errors with detailed information:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Seconds—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Count—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- State—State of the error. Any state other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- BIP-B2—Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- REI-L—Remote error indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- RDI-L—Remote defect indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- AIS-L—Alarm indication signal (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- BERR-SF—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- BERR-SD—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ES-L—Errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SES-L—Severely errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- UAS-L—Unavailable seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ES-LFE—Errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- SES-LFE—Severely errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- UAS-LFE—Unavailable seconds (far-end line)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 41: show interfaces (Gigabit Ethernet) 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>WIS path</strong></td>
<td>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. Any state other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B3</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-P</strong>—Remote error indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOP-P</strong>—Loss of pointer (path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-P</strong>—Path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-P</strong>—Path remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UNEQ-P</strong>—Path unequipped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLM-P</strong>—Path payload (signal) label mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-P</strong>—Errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-P</strong>—Severely errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-P</strong>—Unavailable seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-PFE</strong>—Severely errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-PFE</strong>—Unavailable seconds (far-end STS path)</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation information</td>
<td>Information about link autonegotiation.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Negotiation status:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Incomplete</strong>—Ethernet interface has the speed or link mode configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>No autonegotiation</strong>—Remote Ethernet interface has the speed or link mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured, or does not perform autonegotiation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong>—Ethernet interface is connected to a device that performs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner status</strong>—OK when Ethernet interface is connected to a device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner</strong>—Information from the remote Ethernet device:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link mode</strong>—Depending on the capability of the link partner, either</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full-duplex or Half-duplex.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Types of flow control supported by the link partner. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet interfaces, types are <strong>Symmetric</strong> (link partner supports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAUSE on receive and transmit), <strong>Asymmetric</strong> (link partner supports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAUSE on transmit), <strong>Symmetric/Asymmetric</strong> (link partner supports PAUSE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on receive and transmit or only PAUSE on transmit), and <strong>None</strong> (link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>partner does not support flow control).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information from the link partner—<strong>Failure</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates a receive link error. <strong>OK</strong> indicates that the link partner is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receiving. <strong>Negotiation error</strong> indicates a negotiation error. <strong>Offline</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates that the link partner is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local resolution</strong>—Information from the local Ethernet device:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Types of flow control supported by the local device. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet interfaces, advertised capabilities are *<em>Symmetric</em>/</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Asymmetric</strong> (local device supports PAUSE on receive and transmit or only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAUSE on receive) and <strong>None</strong> (local device does not support flow control).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Depending on the result of the negotiation with the link partner, local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>resolution flow control type will display <strong>Symmetric</strong> (local device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supports PAUSE on receive and transmit), <strong>Asymmetric</strong> (local device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supports PAUSE on receive), and <strong>None</strong> (local device does not support flow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>control).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information. <strong>Link OK</strong> (no error detected on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receive), <strong>Offline</strong> (local interface is offline), and <strong>Link Failure</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(link error detected on receive).</td>
<td></td>
</tr>
<tr>
<td>Received path trace,</td>
<td>Received path trace, Transmitted path trace: (10-Gigabit Ethernet interfaces,</td>
<td>extensive</td>
</tr>
<tr>
<td>Transmitted path trace</td>
<td>WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband</td>
<td></td>
</tr>
<tr>
<td></td>
<td>across the SONET/SDH link. Juniper Networks and other router manufacturers use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>these bytes to help diagnose misconfigurations and network errors by setting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the transmitted path trace message so that it contains the system hostname and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>name of the physical interface. The received path trace value is the message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>received from the router at the other end of the fiber. The transmitted path</td>
<td></td>
</tr>
<tr>
<td></td>
<td>trace value is the message that this router transmits.</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding Engine</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td>configuration</td>
<td>• <strong>Destination slot</strong>—FPC slot number.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 41: show interfaces (Gigabit Ethernet) 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>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>• CoS transmit queue</td>
<td>Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth %</td>
<td>Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth bps</td>
<td>Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td>• Buffer %</td>
<td>Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Buffer usec</td>
<td>Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td>• Priority</td>
<td>Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td>• Limit</td>
<td>Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

### Logical Interface

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Description</th>
<th>Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 41: `show interfaces (Gigabit Ethernet)` 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>VLAN-Tag</strong></td>
<td>Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pop—The outer VLAN tag of the incoming frame is removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>swap—The outer VLAN tag of the incoming frame is overwritten with the user-specified VLAN tag information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>push-push—Two VLAN tags are pushed in from the incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>swap-push—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>swap-swap—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user-specified VLAN tag value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pop-swap—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pop-pop—Both the outer and inner VLAN tags of the incoming frame are removed.</td>
<td></td>
</tr>
<tr>
<td><strong>Demux</strong></td>
<td>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>Source Family Inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination Family Inet</td>
<td></td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>ACI VLAN</strong></td>
<td>Information displayed for agent circuit identifier (ACI) interface set configured with the <code>agent-circuit-id</code> autoconfiguration stanza.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>Dynamic Profile—Name of the dynamic profile that defines the ACI interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If configured, the ACI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ACI information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: The ACI VLAN field is replaced with the Line Identity field when an ALI interface set is configured with the <code>line-identity</code> autoconfiguration stanza.</td>
<td></td>
</tr>
<tr>
<td><strong>Line Identity</strong></td>
<td>Information displayed for access-line-identifier (ALI) interface sets configured with the <code>line-identity</code> autoconfiguration stanza.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>Dynamic Profile—Name of the dynamic profile that defines the ALI interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trusted option used to create the ALI interface set: Circuit-id, Remote-id, or Accept-no-ids. More than one option can be configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If configured, the ALI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ALI information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: The Line Identity field is replaced with the ACI VLAN field when an ACI interface set is configured with the <code>agent-circuit-id</code> autoconfiguration stanza.</td>
<td></td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol family. Possible values are described in the “Protocol Field” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
  - Max nh cache—Maximum interface neighbor discovery nexthop cache size.  
  - New hold nh limit—Maximum number of new unresolved nexthops.  
  - Curr nh cnt—Current number of resolved nexthops in the NDP queue.  
  - Curr new hold cnt—Current number of unresolved nexthops in the NDP queue.  
  - NH drop cnt—Number of NDP requests not serviced. | All levels |
| Dynamic Profile             | Name of the dynamic profile that was used to create this interface configured with a Point-to-Point Protocol over Ethernet (PPPoE) family. | detail extensive none |
| Service Name Table          | Name of the service name table for the interface configured with a PPPoE family. | detail extensive none |
| Max Sessions                | Maximum number of PPPoE logical interfaces that can be activated on the underlying interface. | detail extensive none |
| Duplicate Protection        | State of PPPoE duplicate protection: On or Off. When duplicate protection is configured for the underlying interface, a dynamic PPPoE logical interface cannot be activated when an existing active logical interface is present for the same PPPoE client. | detail extensive none |
| Direct Connect              | State of the configuration to ignore DSL Forum VSAs: On or Off. When configured, the router ignores any of these VSAs received from a directly connected CPE device on the interface. | detail extensive none |
| AC Name                     | Name of the access concentrator.                                                  | detail extensive none |
| Maximum labels              | Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface. | detail extensive none |
| Traffic statistics          | Number and rate of bytes and packets received and transmitted on the specified interface set.  
  - Input bytes, Output bytes—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.  
  - Input packets, Output packets—Number of packets received and transmitted on the interface set. | detail extensive |
| IPv6 transit statistics     | Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled. | extensive |
| Local statistics            | Number and rate of bytes and packets destined to the router.                     | extensive |
### Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the <strong>Output bytes</strong> and <strong>Output packets</strong> interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.</td>
<td></td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the <strong>“Family Flags”</strong> section under <strong>“Common Output Fields Description”</strong> on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Donor interface</td>
<td>(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Preferred source address</td>
<td>(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mac-Validate Failures</td>
<td>Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the <strong>“Addresses Flags”</strong> section under <strong>“Common Output Fields Description”</strong> on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the address flag. Possible values are described in the <strong>“Addresses Flags”</strong> section under <strong>“Common Output Fields Description”</strong> on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 41: show interfaces (Gigabit Ethernet) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

The following table describes the output fields for the **show interfaces** (10–Gigabit Ethernet) command.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of loopback: <strong>Local</strong> or <strong>Remote</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>LAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.</td>
<td>All levels</td>
</tr>
<tr>
<td>WAN-PHY mode</td>
<td>10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unidirectional</td>
<td>Unidirectional link mode status for 10-Gigabit Ethernet interface: <strong>Enabled</strong> or <strong>Disabled</strong> for parent interface; <strong>Rx-only</strong> or <strong>Tx-only</strong> for child interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Auto-negotiation</td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Levels</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Remote-fault</td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Wavelength</td>
<td>(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).</td>
<td>All levels</td>
</tr>
<tr>
<td>Frequency</td>
<td>(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).</td>
<td>All levels</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Schedulers</td>
<td>(Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces only) Number of CoS schedulers configured.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is <em>Last flapped: year-month-day hour:minute:second:timezone</em> <em>(hour:minute:second ago).</em> For example, <em>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</em></td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps). The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td>None specified</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Egress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for egress traffic.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Ingress account overhead</td>
<td>Layer 2 overhead in bytes that is accounted in the interface statistics for ingress traffic.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Traffic statistics

Number and rate of bytes and packets received and transmitted on the physical interface.

- **Input bytes**—Number of bytes received on the interface. The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.
- **Output bytes**—Number of bytes transmitted on the interface. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.
- **Input packets**—Number of packets received on the interface.
- **Output packets**—Number of packets transmitted on the interface.

### Input errors

Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:

- **Errors**—Sum of the incoming frame aborts and FCS errors.
- **Drops**—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.
- **Framing errors**—Number of packets received with an invalid frame checksum (FCS).
- **Runt**—Number of frames received that are smaller than the runt threshold.
- **Policed discards**—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.
- **L3 incompletes**—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the `ignore-l3-incompletes` statement.
- **L2 channel errors**—Number of times the software did not find a valid logical interface for an incoming frame.
- **L2 mismatch timeouts**—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.
- **FIFO errors**—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.
- **Resource errors**—Sum of transmit drops.
### Output errors

Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:

- **Carrier transitions**—Number of times the interface has gone from **down** to **up**. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.

- **Errors**—Sum of the outgoing frame aborts and FCS errors.

- **Drops**—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.

- **Collisions**—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.

- **Aged packets**—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.

- **FIFO errors**—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.

- **HS link CRC errors**—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.

- **MTU errors**—Number of packets whose size exceeded the MTU of the interface.

- **Resource errors**—Sum of transmit drops.

### Egress queues

Total number of egress queues supported on the specified interface.

**NOTE:** In DPCs that are not of the enhanced type, such as DPC 40x1GE R, DPCE 20x1GE + 2x10GE R, or DPCE 40x1GE R, you might notice a discrepancy in the output of the `show interfaces` command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs.

### Queue counters (Egress)

CoS queue number and its associated user-configured forwarding class name.

- **Queued packets**—Number of queued packets.

- **Transmitted packets**—Number of transmitted packets.

- **Dropped packets**—Number of packets dropped by the ASIC’s RED mechanism.

### Ingress queues

Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.
### Queue counters (Ingress)

CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces.

- **Queued packets**—Number of queued packets.
- **Transmitted packets**—Number of transmitted packets.
- **Dropped packets**—Number of packets dropped by the ASIC's RED mechanism.

### Active alarms and Active defects

Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the routing device configuration, an alarm can ring the red or yellow alarm bell on the routing device, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value **None** or **Link**.

- **None**—There are no active defects or alarms.
- **Link**—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.

### OTN alarms

Active OTN alarms identified on the interface.

### OTN defects

OTN defects received on the interface.

### OTN FEC Mode

The FEC mode configured on the interface.

- **efec**—Enhanced forward error correction (EFEC) is configured to detect and correct bit errors.
- **gfec**—G.709 Forward error correction (GFEC) mode is configured to detect and correct bit errors.
- **none**—FEC mode is not configured.

### OTN Rate

OTN mode.

- **fixed-stuff-bytes**—Fixed stuff bytes 11.0957 Gbps.
- **no-fixed-stuff-bytes**—No fixed stuff bytes 11.0491 Gbps.
- **pass-through**—Enable OTN passthrough mode.
- **no-pass-through**—Do not enable OTN passthrough mode.

### OTN Line Loopback

Status of the line loopback, if configured for the DWDM OTN PIC. Its value can be: **enabled** or **disabled**.

### OTN FEC statistics

The forward error correction (FEC) counters for the DWDM OTN PIC.

- **Corrected Errors**—The count of corrected errors in the last second.
- **Corrected Error Ratio**—The corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits.

### OTN FEC alarms

OTN FEC excessive or degraded error alarms triggered on the interface.

- **FEC Degradate**—OTU FEC Degradate defect.
- **FEC Excessive**—OTU FEC Excessive Error defect.
OTN OC | OTN OC defects triggered on the interface.
---|---
• LOS—OC Loss of Signal defect.
• LOF—OC Loss of Frame defect.
• LOM—OC Loss of Multiframe defect.
• Wavelength Lock—OC Wavelength Lock defect.

OTN OTU | OTN OTU defects detected on the interface
---|---
• AIS—OTN AIS alarm.
• BDI—OTN OTU BDI alarm.
• IAE—OTN OTU IAE alarm.
• TTIM—OTN OTU TTIM alarm.
• SF—OTN ODU bit error rate fault alarm.
• SD—OTN ODU bit error rate defect alarm.
• TCA-ES—OTN ODU ES threshold alarm.
• TCA-SES—OTN ODU SES threshold alarm.
• TCA-UAS—OTN ODU UAS threshold alarm.
• TCA-BBE—OTN ODU BBE threshold alarm.
• BIP—OTN ODU BIP threshold alarm.
• BBE—OTN OTU BBE threshold alarm.
• ES—OTN OTU ES threshold alarm.
• SES—OTN OTU SES threshold alarm.
• UAS—OTN OTU UAS threshold alarm.

Received DAPI | Destination Access Port Interface (DAPI) from which the packets were received.
---|---

Received SAPI | Source Access Port Interface (SAPI) from which the packets were received.
---|---

Transmitted DAPI | Destination Access Port Interface (DAPI) to which the packets were transmitted.
---|---

Transmitted SAPI | Source Access Port Interface (SAPI) to which the packets were transmitted.
---|---

PCS statistics | (10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.
---|---
• Bit errors—The number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.
• Errored blocks—The number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.
MAC statistics

Receive and Transmit statistics reported by the PIC’s MAC subsystem, including the following:

- **Total octets and total packets**—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type.
- **Unicast packets, Broadcast packets, and Multicast packets**—Number of unicast, broadcast, and multicast packets.
- **CRC/Align errors**—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
- **FIFO error**—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.
- **MAC control frames**—Number of MAC control frames.
- **MAC pause frames**—Number of MAC control frames with pause operational code.
- **Oversized frames**—Number of frames that exceed 1518 octets.
- **Jabber frames**—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.
- **Fragment frames**—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.
- **VLAN tagged frames**—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.
- **Code violations**—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”

<table>
<thead>
<tr>
<th>OTN Received Overhead Bytes</th>
<th>APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTN Transmitted Overhead Bytes</td>
<td>APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Filter statistics

Receive and Transmit statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet should enter the system or be rejected.

- **Input packet count**—Number of packets received from the MAC hardware that the filter processed.
- **Input packet rejects**—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.
- **Input DA rejects**—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the routing device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local routing device (which the routing device is rejecting).
- **Input SA rejects**—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.
- **Output packet count**—Number of packets that the filter has given to the MAC hardware.
- **Output packet pad count**—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.
- **Output packet error count**—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.
- **CAM destination filters, CAM source filters**—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0.

PMA PHY

(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:

- **Seconds**—Number of seconds the defect has been active.
- **Count**—Number of times that the defect has gone from inactive to active.
- **State**—State of the error. Any state other than **OK** indicates a problem.
**WIS section**  
(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:  
- **Seconds**—Number of seconds the defect has been active.  
- **Count**—Number of times that the defect has gone from inactive to active.  
- **State**—State of the error. Any state other than *OK* indicates a problem.  

Subfields are:  
- **BIP-B1**—Bit interleaved parity for SONET section overhead  
- **SEF**—Severely errored framing  
- **LOL**—Loss of light  
- **LOF**—Loss of frame  
- **ES-S**—Errored seconds (section)  
- **SES-S**—Severely errored seconds (section)  
- **SEFS-S**—Severely errored framing seconds (section)

**WIS line**  
(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:  
- **Seconds**—Number of seconds the defect has been active.  
- **Count**—Number of times that the defect has gone from inactive to active.  
- **State**—State of the error. State other than *OK* indicates a problem.  

Subfields are:  
- **BIP-B2**—Bit interleaved parity for SONET line overhead  
- **REI-L**—Remote error indication (near-end line)  
- **RDI-L**—Remote defect indication (near-end line)  
- **AIS-L**—Alarm indication signal (near-end line)  
- **BERR-SF**—Bit error rate fault (signal failure)  
- **BERR-SD**—Bit error rate defect (signal degradation)  
- **ES-L**—Errored seconds (near-end line)  
- **SES-L**—Severely errored seconds (near-end line)  
- **UAS-L**—Unavailable seconds (near-end line)  
- **ES-LFE**—Errored seconds (far-end line)  
- **SES-LFE**—Severely errored seconds (far-end line)  
- **UAS-LFE**—Unavailable seconds (far-end line)
### Interface Operational Commands

#### WIS path

(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.

- **Seconds**—Number of seconds the defect has been active.
- **Count**—Number of times that the defect has gone from inactive to active.
- **State**—State of the error. Any state other than **OK** indicates a problem.

Subfields are:

- **BIP-B3**—Bit interleaved parity for SONET section overhead
- **REI-P**—Remote error indication
- **LOP-P**—Loss of pointer (path)
- **AIS-P**—Path alarm indication signal
- **RDI-P**—Path remote defect indication
- **UNEQ-P**—Path unequipped
- **PLM-P**—Path payload label mismatch
- **ES-P**—Errored seconds (near-end STS path)
- **SES-P**—Severely errored seconds (near-end STS path)
- **UAS-P**—Unavailable seconds (near-end STS path)
- **SES-PFE**—Severely errored seconds (far-end STS path)
- **UAS-PFE**—Unavailable seconds (far-end STS path)

#### Autonegotiation information

Information about link autonegotiation.

- **Negotiation status:**
  - **Incomplete**—Ethernet interface has the speed or link mode configured.
  - **No autonegotiation**—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.
  - **Complete**—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.

- **Link partner status**—**OK** when Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.

- **Link partner:**
  - **Link mode**—Depending on the capability of the attached Ethernet device, either **Full-duplex** or **Half-duplex**.
  - **Flow control**—Types of flow control supported by the remote Ethernet device. For Fast Ethernet interfaces, the type is **None**. For Gigabit Ethernet interfaces, types are **Symmetric** (link partner supports **PAUSE** on receive and transmit), **Asymmetric** (link partner supports **PAUSE** on transmit), and **Symmetric/Asymmetric** (link partner supports both **PAUSE** on receive and transmit or only **PAUSE** receive).
  - **Remote fault**—Remote fault information from the link partner. **Failure** indicates a receive link error. **OK** indicates that the link partner is receiving. **Negotiation error** indicates a negotiation error. **Offline** indicates that the link partner is going offline.

- **Local resolution**—Information from the link partner:
  - **Flow control**—Types of flow control supported by the remote Ethernet device. For Gigabit Ethernet interfaces, types are **Symmetric** (link partner supports **PAUSE** on receive and transmit), **Asymmetric** (link partner supports **PAUSE** on transmit), and **Symmetric/Asymmetric** (link partner supports both **PAUSE** on receive and transmit or only **PAUSE** receive).
  - **Remote fault**—Remote fault information. **Link OK** (no error detected on receive), **Offline** (local interface is offline), and **Link Failure** (link error detected on receive).
Received path trace, Transmitted path trace

(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.

Packet Forwarding Engine configuration

Information about the configuration of the Packet Forwarding Engine:
- **Destination slot**—FPC slot number.

CoS information

Information about the CoS queue for the physical interface.
- **CoS transmit queue**—Queue number and its associated user-configured forwarding class name.
- **Bandwidth %**—Percentage of bandwidth allocated to the queue.
- **Bandwidth bps**—Bandwidth allocated to the queue (in bps).
- **Buffer %**—Percentage of buffer space allocated to the queue.
- **Buffer usec**—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.
- **Priority**—Queue priority: low or high.
- **Limit**—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.

Logical Interface

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### VLAN-Tag
Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.

- **push**—An outer VLAN tag is pushed in front of the existing VLAN tag.
- **pop**—The outer VLAN tag of the incoming frame is removed.
- **swap**—The outer VLAN tag of the incoming frame is overwritten with the user specified VLAN tag information.
- **push**—An outer VLAN tag is pushed in front of the existing VLAN tag.
- **push-push**—Two VLAN tags are pushed in from the incoming frame.
- **swap-push**—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.
- **swap-swap**—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user specified VLAN tag value.
- **pop-swap**—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.
- **pop-pop**—Both the outer and inner VLAN tags of the incoming frame are removed.

### Demux:
IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:

- Source Family Inet
- Destination Family Inet

### Encapsulation
Encapsulation on the logical interface.

### Protocol
Protocol family. Possible values are described in the “Protocol Field” section under “Common Output Fields Description” on page 1152.

### MTU
Maximum transmission unit size on the logical interface.

### Maximum labels
Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.

### Traffic statistics
Number and rate of bytes and packets received and transmitted on the specified interface set.

- **Input bytes, Output bytes**—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.
- **Input packets, Output packets**—Number of packets received and transmitted on the interface set.

### IPv6 transit statistics
Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.

### Local statistics
Number and rate of bytes and packets destined to the routing device.
**Transit statistics**  Number and rate of bytes and packets transiting the switch.

*NOTE:* For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the *Output bytes* and *Output packets* interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.

| **Generation** | Unique number for use by Juniper Networks technical support only. | detail extensive |
| **Route Table** | Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0. | detail extensive none |
| **Flags** | Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152. | detail extensive |
| **Donor interface** | (Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address. | detail extensive none |
| **Preferred source address** | (Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface. | detail extensive none |
| **Input Filters** | Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces. | detail extensive |
| **Output Filters** | Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces. | detail extensive |
| **Mac-Validate Failures** | Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface. | detail extensive none |
| **Addresses, Flags** | Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152. | detail extensive none |
| **protocol-family** | Protocol family configured on the logical interface. If the protocol is *inet*, the IP address of the interface is also displayed. | brief |
| **Flags** | Information about address flag (possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152. | detail extensive none |
| **Destination** | IP address of the remote side of the connection. | detail extensive none |
| **Local** | IP address of the logical interface. | detail extensive none |
| **Broadcast** | Broadcast address of the logical interface. | detail extensive none |
| **Generation** | Unique number for use by Juniper Networks technical support only. | detail extensive |
For Gigabit Ethernet IQ PICs, traffic and MAC statistics output varies. The following table describes the traffic and MAC statistics for two sample interfaces, each of which is sending traffic in packets of 500 bytes (including 478 bytes for the Layer 3 packet, 18 bytes for the Layer 2 VLAN traffic header, and 4 bytes for cyclic redundancy check [CRC] information). The `ge-0/3/0` interface is the inbound physical interface, and the `ge-0/0/0` interface is the outbound physical interface. On both interfaces, traffic is carried on logical unit .50 (VLAN 50).

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Sample Command</th>
<th>Byte and Octet Counts Include</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound physical interface</td>
<td><code>show interfaces ge-0/3/0 extensive</code></td>
<td>Traffic statistics:</td>
<td>The additional 4 bytes are for the CRC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 496 bytes per packet, representing the Layer 2 packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Received octets: 500 bytes per packet, representing the Layer 2 packet + 4 bytes</td>
<td></td>
</tr>
<tr>
<td>Inbound logical interface</td>
<td><code>show interfaces ge-0/3/0.50 extensive</code></td>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
<tr>
<td>Outbound physical interface</td>
<td><code>show interfaces ge-0/0/0 extensive</code></td>
<td>Traffic statistics:</td>
<td>For input bytes, the additional 12 bytes include 6 bytes for the destination MAC address plus 4 bytes for VLAN plus 2 bytes for the Ethernet type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 490 bytes per packet, representing the Layer 3 packet + 12 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Received octets: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
<tr>
<td>Outbound logical interface</td>
<td><code>show interfaces ge-0/0/0.50 extensive</code></td>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Input bytes: 478 bytes per packet, representing the Layer 3 packet</td>
<td></td>
</tr>
</tbody>
</table>

Table 32 on page 1196 lists the output fields for the `show interfaces` command. Output fields are listed in the approximate order in which they appear.
### Table 43: show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface index</strong></td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td><strong>Link-level type</strong></td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Link mode</strong></td>
<td>Link mode: Full-duplex or Half-duplex.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>BPDU error</strong></td>
<td>Bridge protocol data unit (BPDU) error: Detected or None</td>
<td></td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of loopback:</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Source filtering</strong></td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Flow control</strong></td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Auto-negotiation</strong></td>
<td>(Gigabit Ethernet interfaces) Autonegotiation status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Remote-fault</strong></td>
<td>(Gigabit Ethernet interfaces) Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- <strong>Online</strong>—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Offline</strong>—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td><strong>Device flags</strong></td>
<td>Information about the physical device.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface flags</strong></td>
<td>Information about the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Link flags</strong></td>
<td>Information about the physical link.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td><strong>Current address</strong></td>
<td>Configured MAC address.</td>
<td>detail extensive, none</td>
</tr>
</tbody>
</table>
### Table 43: show 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><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: <em>year-month-day</em> <em>hour:minute:second</em> <em>timezone</em> (<em>hour:minute:second ago</em>). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td><strong>Input Rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None</td>
</tr>
<tr>
<td><strong>Output Rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Active alarms and Active defects</strong></td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. These fields can contain the value None or Link.</td>
<td>detail extensive, none</td>
</tr>
<tr>
<td>• <strong>None</strong>—There are no active defects or alarms.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Link</strong>—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 43: show 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><strong>Input errors</strong></td>
<td>Input errors on the interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L3 incompletes</strong>—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the <code>ignore-l3-incompletes</code> .</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 channel errors</strong>—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>L2 mismatch timeouts</strong>—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Collisions</strong>—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation; therefore, for Gigabit Ethernet PICs, this number must always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field must never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 43: show 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>Ingress queues</td>
<td>Total number of ingress queues supported on the specified interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Queue counters and queue number</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
</tbody>
</table>

MAC statistics

Receive and Transmit statistics reported by the PIC’s MAC subsystem, including the following:

- **Total octets and total packets**—Total number of octets and packets.
- **Unicast packets, Broadcast packets, and Multicast packets**—Number of unicast, broadcast, and multicast packets.
- **CRC/Align errors**—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
- **FIFO error**—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.
- **MAC control frames**—Number of MAC control frames.
- **MAC pause frames**—Number of MAC control frames with pause operational code.
- **Oversized frames**—There are two possible conditions regarding the number of oversized frames:
  - Packet length exceeds 1518 octets, or
  - Packet length exceeds MRU
- **Jabber frames**—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.
- **Fragment frames**—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.
- **VLAN tagged frames**—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.
- **Code violations**—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”
Table 43: show 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>Filter statistics</td>
<td>Receive and Transmit statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packet count — Number of packets received from the MAC hardware that the filter processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packet rejects — Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input DA rejects — Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local device (which the router is rejecting).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input SA rejects — Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packet count — Number of packets that the filter has given to the MAC hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packet pad count — Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packet error count — Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CAM destination filters, CAM source filters — Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields must be 0.</td>
<td></td>
</tr>
</tbody>
</table>

Autonegotiation information

Information about link autonegotiation. extensive

• Negotiation status:
  • Incomplete — Ethernet interface has the speed or link mode configured.
  • No autonegotiation — Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation.
  • Complete — Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful.

Packet Forwarding Engine configuration

Information about the configuration of the Packet Forwarding Engine: extensive

• Destination slot — FPC slot number.
<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Field Description</strong></th>
<th><strong>Level of Output</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
<tr>
<td>Interface transmit statistics</td>
<td>Status of the interface-transmit-statistics configuration: Enabled or Disabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Queue counters (Egress)</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the specified interface set.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes, Output bytes—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets, Output packets—Number of packets received and transmitted on the interface set.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 43: show 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>Local statistics</td>
<td>Number and rate of bytes and packets destined to the device.</td>
<td>extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the Output bytes and Output packets interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Security zones that interface belongs to.</td>
<td>extensive</td>
</tr>
<tr>
<td>Flow Input statistics</td>
<td>Statistics on packets received by flow module.</td>
<td>extensive</td>
</tr>
<tr>
<td>Flow Output statistics</td>
<td>Statistics on packets sent by flow module.</td>
<td>extensive</td>
</tr>
<tr>
<td>Flow error statistics (Packets dropped due to)</td>
<td>Statistics on errors in the flow module.</td>
<td>extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Sample Output Gigabit Ethernet

show interfaces (Gigabit Ethernet)

```
user@host> show interfaces ge-3/0/2

Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Interface index: 167, SNMP ifIndex: 35
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Remote fault: Online
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues : 4 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
  Last flapped : 2006-08-10 17:25:10 PDT (00:01:08 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  Ingress rate at Packet Forwarding Engine : 0 bps (0 pps)
  Ingress drop rate at Packet Forwarding Engine : 0 bps (0 pps)
  Active alarms : None
  Active defects : None

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69)
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push 0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
  Egress account overhead: 100
  Ingress account overhead: 90
  Input packets: 0
  Output packets: 0
  Protocol ccc, MTU: 1522
  Flags: Is-Primary
```

show interfaces (Gigabit Ethernet on MX Series Routers)

```
user@host> show interfaces ge-2/2/2

Physical interface: ge-2/2/2, Enabled, Physical link is Up
  Interface index: 156, SNMP ifIndex: 188
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, MAC-REWRITE Error: None,
  Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 4 maximum usable queues
  Schedulers : 0
  Current address: 00:00:5e:00:53:c0, Hardware address: 00:00:5e:00:53:76
  Last flapped : 2008-09-05 16:44:30 PDT (3d 01:04 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  Active alarms : None
  Active defects : None

Logical interface ge-2/2/2.0 (Index 82) (SNMP ifIndex 219)
  Flags: Up SNMP-Traps 0x4004000 Encapsulation: ENET2
  Input packets: 10232
  Output packets: 10294
```
show interfaces (link degrade status)

```bash
user@host> show interfaces et-3/0/0
```

| Physical interface: et-3/0/0, Enabled, Physical link is Down |
| Interface index: 157, SNMP ifIndex: 537 |
| Link-level type: Ethernet, MTU: 1514, MRU: 0, Speed: 100Gbps, BPDU Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled |
| Device flags : Present Running Down |
| Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000 |
| Link flags : None |
| CoS queues : 8 supported, 8 maximum usable queues |
| Current address: 54:e0:32:23:9d:38, Hardware address: 54:e0:32:23:9d:38 |
| Last flapped : 2014-06-18 02:36:38 PDT (02:50:50 ago) |
| Input rate : 0 bps (0 pps) |
| Output rate : 0 bps (0 pps) |
| Active alarms : LINK |
| Active defects : LINK |
| PCS statistics Seconds |
| Bit errors : 0 |
| Errored blocks : 0 |
| Link Degradation : Enable |
| Link Monitoring : 1E-7 |
| Link Degradation Set Threshold: : 1E-12 |
| Link Degradation Clear Threshold: : 1E-7 |
| Estimated BER : |
| Link-degrade event : Seconds Count State |
| 782 1 Defect Active |

show interfaces extensive (Gigabit Ethernet on MX Series Routers showing interface transmit statistics configuration)

```bash
user@host> show interfaces ge-2/1/2 extensive | match "output|interface"
```

| Physical interface: ge-2/1/2, Enabled, Physical link is Up |
| Interface index: 151, SNMP ifIndex: 530, Generation: 154 |
| Interface flags: SNMP-Traps Internal: 0x4000 |
| Output bytes : 240614363944 772721536 bps |
| Output packets: 3538446506 1420444 pps |
| Direction : Output |
| Interface transmit statistics: Enabled |

Logical interface ge-2/1/2.0 (Index 331) (SNMP ifIndex 955) (Generation 146)
show interfaces ge-3/0/2 brief

user@host> show interfaces ge-3/0/2 brief

Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : None

Logical interface ge-3/0/2.0
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push 0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC

Logical interface ge-3/0/2.32767
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2

show interfaces detail (Gigabit Ethernet)

user@host> show interfaces ge-3/0/2 detail
Physical interface: ge-3/0/2, Enabled, Physical link is Up
Interface index: 167, SNMP ifIndex: 35, Generation: 177
Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
Source Filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 4 supported, 4 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
Last flapped : 2006-08-09 17:17:00 PDT (01:31:33 ago)
Statistics last cleared: Never
Traffic statistics:
<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Input bytes</th>
<th>Output bytes</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Ingress traffic statistics at Packet Forwarding Engine:
<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress traffic statistics at Packet Forwarding Engine:
<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69) (Generation 140)
Flags: SNMP-Traps 0x4000
VLAN-Tag [0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530)
Out(swap-push 0x8100.512 0x8100.513)
Encapsulation: VLAN-CCC
Egress account overhead: 100
Ingress account overhead: 90
Traffic statistics:
<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Input bytes</th>
<th>Output bytes</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Protocol ccc, MTU: 1522, Generation: 149, Route table: 0
Flags: Is-Primary

Logical interface ge-3/0/2.32767 (Index 71) (SNMP ifIndex 70)
(Generation 139)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

show interfaces extensive (Gigabit Ethernet iQ2)

user@host> show interfaces ge-7/1/3 extensive

Physical interface: ge-7/1/3, Enabled, Physical link is Up
Interface index: 170, SNMP ifIndex: 70, Generation: 171
Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
Source Filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000000
Link flags : None
CoS queues : 8 supported, 4 maximum usable queues
Schedulers : 256
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:74, Hardware address: 00:00:5e:00:53:74
Statistics last cleared: Never
Traffic statistics:
Input bytes : 38910844056 7952 bps
Output bytes : 7174605 8464 bps
Input packets: 418398473 11 pps
Output packets: 78903 12 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Ingress traffic statistics at Packet Forwarding Engine:

Input  bytes  : 38910799145  7952 bps
Input  packets: 418397956  11 pps
Drop   bytes  : 0  0 bps
Drop   packets: 0  0 pps

Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0

Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Ingress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>418390823</td>
<td>418390823</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>7133</td>
<td>7133</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>1031</td>
<td>1031</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>77872</td>
<td>77872</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms  : None
Active defects  : None

MAC statistics: Receive  Transmit
Total octets  38910844056  7174605
Total packets 418398473  78903
Unicast packets 408021893366  1026
Broadcast packets 10  12
Multicast packets 418398217  77865
CRC/Align errors 0  0
FIFO errors 0  0
MAC control frames 0  0
MAC pause frames 0  0
Oversized frames 0
Jabber frames 0
Fragment frames 0
VLAN tagged frames 0
Code violations 0

OTN Received Overhead Bytes: APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58
Payload Type: 0x08

OTN Transmitted Overhead Bytes: APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
Payload Type: 0x08

Filter statistics:
Input packet count 418398473
Input packet rejects 479
Input DA rejects                       479
Input SA rejects                         0
Output packet count                                   78903
Output packet pad count                                   0
Output packet error count                                 0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: Symmetric/Asymmetric,
    Remote fault: OK
Local resolution:
  Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
  Destination slot: 7
CoS information:
  Direction : Output
    CoS transmit queue          Bandwidth          Buffer     Priority   Limit
       %            bps     %           usec
 0 best-effort            95      950000000    95              0
  low    none
    3 network-control         5       50000000     5              0
  low    none
Direction : Input
    CoS transmit queue          Bandwidth          Buffer     Priority   Limit
       %            bps     %           usec
 0 best-effort            95      950000000    95              0
  low    none
    3 network-control         5       50000000     5              0
  low    none
Logical interface ge-7/1/3.0 (Index 70) (SNMP ifIndex 85) (Generation 150)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes :               812400
  Output bytes :              1349206
  Input packets:                 9429
  Output packets:                 9449
IPV6 transit statistics:
  Input bytes :                   0
  Output bytes :                   0
  Input packets:                   0
  Output packets:                   0
Local statistics:
  Input bytes :               812400
  Output bytes :              1349206
  Input packets:                 9429
  Output packets:                 9449
Transit statistics:
  Input bytes :                   0                 7440 bps
  Output bytes :                   0                 7888 bps
  Input packets:                   0                   10 pps
  Output packets:                   0                   11 pps
IPV6 transit statistics:
  Input bytes :                   0
  Output bytes :                   0
  Input packets:                   0
  Output packets:                   0
Protocol inet, MTU: 1500, Generation: 169, Route table: 0
  Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
Input Filters: F1-ge-3/0/1.0-in, F3-ge-3/0/1.0-in
Output Filters: F2-ge-3/0/1.0-out (53)
Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 203.0.113.255,
Generation: 196
Protocol multiservice, MTU: Unlimited, Generation: 170, Route table: 0
Flags: Is-Primary
Policer: Input: __default_arp_policer_

NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface
egress statistics displayed in the show interfaces command output might not accurately
reflect the traffic on the wire when output shaping is applied. Traffic management output
shaping might drop packets after they are tallied by the interface counters. For detailed
information, see the description of the logical interface Transit statistics fields in
Table 30 on page 1166.

show interfaces (Gigabit Ethernet Unnumbered Interface)

user@host> show interfaces ge-3/2/0
Physical interface: ge-3/2/0, Enabled, Physical link is Up
  Interface index: 148, SNMP ifIndex: 50
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:f8, Hardware address: 00:00:5e:00:53:f8
  Last flapped : 2006-10-27 04:42:23 PDT (08:01:52 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 624 bps (1 pps)
  Active alarms : None
  Active defects : None

Logical interface ge-3/2/0.0 (Index 67) (SNMP ifIndex 85)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 0
  Output packets: 6
  Protocol inet, MTU: 1500
  Flags: Unnumbered
  Donor interface: lo0.0 (Index 64)
  Preferred source address: 203.0.113.22

show interfaces (ACI Interface Set Configured)

user@host> show interfaces ge-1/0/0.4001
Logical interface ge-1/0/0.4001 (Index 340) (SNMP ifIndex 548)
  Flags: SNMP-Traps Encapsulation: PPP-over-
  Ethernet
  ACI VLAN:
  Dynamic Profile: aci-vlan-set-profile
  PPPoE:
Dynamic Profile: aci-vlan-pppoe-profile,
Service Name Table: None,
Max Sessions: 32000, Max Sessions VSA Ignore: Off,
Duplicate Protection: On, Short Cycle Protection: Off,
Direct Connect: Off,
AC Name: nbc
Input packets : 9
Output packets: 8
Protocol multiservice, MTU: Unlimited

show interfaces (ALI Interface Set)

user@host> show interfaces ge-1/0/0.10
Logical interface ge-1/0/0.10 (Index 346) (SNMP ifIndex 554) (Generation 155)
  Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.10 ] Encapsulation: ENET2
Line Identity:
  Dynamic Profile: ali-set-profile
  Circuit-id Remote-id Accept-no-ids
PPPoE:
  Dynamic Profile: ali-vlan-pppoe-profile,
  Service Name Table: None,
  Max Sessions: 32000, Max Sessions VSA Ignore: Off,
  Duplicate Protection: On, Short Cycle Protection: Off,
  Direct Connect: Off,
  AC Name: nbc
Input packets : 9
Output packets: 8
Protocol multiservice, MTU: Unlimited

Sample Output Gigabit Ethernet

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, IQ2)

user@host> show interfaces xe-5/0/0 extensive
Physical interface: xe-5/0/0, Enabled, Physical link is Up
  Interface index: 177, SNMP ifIndex: 630, Generation: 178
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Speed: 10Gbps, Loopback: None, Source filtering: Enabled,
  Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 4 maximum usable queues
 Schedulers : 1024
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:f6, Hardware address: 00:00:5e:00:53:f6
  Last flapped : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 6970332384  0 bps
    Output bytes : 0  0 bps
    Input packets: 81050506  0 pps
    Output packets: 0  0 pps
  IPv6 transit statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
Output packets: 0

Ingress traffic statistics at Packet Forwarding Engine:

<table>
<thead>
<tr>
<th>Input bytes</th>
<th>6970299398</th>
<th>0 bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packets</td>
<td>81049992</td>
<td>0 pps</td>
</tr>
<tr>
<td>Drop bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Drop packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
</tbody>
</table>

Input errors:
- Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompatibility: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0

Output errors:
- Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Ingress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>81049992</td>
<td>81049992</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms: None
Active defects: None

PCS statistics

| Bit errors | 0 |
| Error blocks | 0 |

MAC statistics:

| Total octets | 6970332384 |
| Total packets | 81050506 |
| Unicast packets | 81050000 |
| Broadcast packets | 506 |
| Multicast packets | 0 |
| CRC/Align errors | 0 |
| FIFO errors | 0 |
| MAC control frames | 0 |
| MAC pause frames | 0 |
| Oversized frames | 0 |
| Jabber frames | 0 |
| Fragment frames | 0 |
| VLAN tagged frames | 0 |
| Code violations | 0 |

Filter statistics:

| Input packet count | 81050506 |
| Input packet rejects | 506 |
| Input DA rejects | 0 |
Logical interface xe-5/0/0.0 (Index 71) (SNMP ifIndex 95) (Generation 195)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ] Encapsulation: ENET2
Egress account overhead: 100
Ingress account overhead: 90
Traffic statistics:
  Input bytes : 0
  Output bytes : 46
  Input packets: 0
  Output packets: 1
IPV6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 46
  Input packets: 0
  Output packets: 1
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
IPV6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Protocol inet, MTU: 1500, Generation: 253, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 192.0.2/24, Local: 192.0.2.1, Broadcast: 192.0.2.255,
  Generation: 265
Protocol multiservice, MTU: Unlimited, Generation: 254, Route table: 0
  Flags: None
  Policer: Input: __default_arp_policer__
Physical interface: xe-1/0/0, Enabled, Physical link is Up  
Interface index: 141, SNMP ifIndex: 630, Generation: 47  
Link-level type: Ethernet, MTU: 1514, Speed: 9.294Gbps, Loopback: Disabled

WAN-PHY mode  
Source filtering: Disabled, Flow control: Enabled Speed Configuration: Auto  
Device flags : Present Running  
Interface flags: SNMP-Traps 16384  
Link flags : None  
CoS queues : 4 supported  
Hold-times : Up 0 ms, Down 0 ms  
Current address: 00:00:5e:00:53:9d, Hardware address: 00:00:5e:00:53:9d  
Statistics last cleared: Never  
Traffic statistics:  
<table>
<thead>
<tr>
<th>Type</th>
<th>In bytes</th>
<th>In pps</th>
<th>Out bytes</th>
<th>Out pps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Input errors:  
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, HS Link CRC errors: 0, HS Link FIFO overflows: 0, Resource errors: 0

Output errors:  
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Queue counters:  
<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms : LOL, LOS,LBL  
Active defects: LOL, LOS,LBL, SEF, AIS-L, AIS-P

PCS statistics:  
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Seconds</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

MAC statistics:  
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:  
<table>
<thead>
<tr>
<th>Statistics</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet count</td>
<td>0</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input SA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Output packet count</td>
<td>0</td>
</tr>
<tr>
<td>Output packet pad count</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces extensive (10-Gigabit Ethernet, DWDM OTN PIC)

```
show interfaces ge-7/0/0 extensive

user@host> show interfaces ge-7/0/0 extensive

Physical interface: ge-7/0/0, Enabled, Physical link is Down
Interface index: 143, SNMP ifIndex: 508, Generation: 208
Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: Ox4000
Link flags : None
Wavelength : 1550.12 nm, Frequency: 193.40 THz
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:72, Hardware address: 00:00:5e:00:53:72
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 2, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 0 0
1 expedited-forw 0 0 0
2 assured-forw 0 0 0
3 network-cont
Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
Active alarms : LINK
Active defects : LINK
MAC statistics: Receive Transmit
Total octets 0 0
Total packets 0 0
Unicast packets 0 0
Broadcast packets 0 0
Multicast packets 0 0
CRC/Align errors 0 0
FIFO errors 0 0
MAC control frames 0 0
MAC pause frames 0 0
Oversized frames 0
Jabber frames 0
Fragment frames 0
VLAN tagged frames 0
Code violations 0
Total octets 0 0
Total packets                            0                0
Unicast packets                          0                0
Broadcast packets                        0                0
Multicast packets                        0                0
CRC/Align errors                         0                0
FIFO errors                              0                0
MAC control frames                       0                0
MAC pause frames                         0                0
Oversized frames                         0
Jabber frames                            0
Fragment frames                          0
VLAN tagged frames                       0
Code violations                          0

OTN alarms : None
OTN defects : None
OTN FEC Mode : GFEC
OTN Rate : Fixed Stuff Bytes 11.0957Gbps
OTN Line Loopback : Enabled
OTN FEC statistics :
  Corrected Errors : 0
  Corrected Error Ratio (0 sec average) : 0e-0

OTN FEC alarms:          Seconds  Count  State
  FEC Degrade              0            0    OK
  FEC Excessive            0            0    OK

OTN OC:          Seconds  Count  State
  LOS                      2            1    OK
  LOF                      67164         2  Defect Active
  LOM                      67164        71  Defect Active
  Wavelength Lock          0            0    OK

OTN OTU:
  AIS                      0            0    OK
  BDI                      65919        4814  Defect Active
  IAE                      67158         1  Defect Active
  TTIM                     7            1    OK
  SF                       67164         2  Defect Active
  SD                       67164         3  Defect Active
  TCA-ES                   0            0    OK
  TCA-SES                  0            0    OK
  TCA-UAS                  80           40    OK
  TCA-BBE                  0            0    OK
  BIP                      0            0    OK
  BBE                      0            0    OK
  ES                       0            0    OK
  SES                      0            0    OK
  UAS                      587          0    OK

Received DAPI:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  

Received SAPI:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  

Transmitted DAPI:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  

Transmitted SAPI:
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ...  

OTN Received Overhead Bytes:
APS/PCC0: 0x02, APS/PCC1: 0x42, APS/PCC2: 0xa2, APS/PCC3: 0x48
Payload Type: 0x03

OTN Transmitted Overhead Bytes:
APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
Payload Type: 0x03

Filter statistics:
show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode)

user@host> show interfaces xe-7/0/0 extensive

Physical interface: xe-7/0/0, Enabled, Physical link is Up
   Interface index: 173, SNMP ifIndex: 212, Generation: 174
   Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
   Unidirectional: Enabled,
   Loopback: None, Source filtering: Disabled, Flow control: Enabled
   Device flags   : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Link flags     : None
   CoS queues     : 8 supported, 8 maximum usable queues
   Hold-times     : Up 0 ms, Down 0 ms
   Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
   Last flapped   : 2007-06-01 09:08:19 PDT (3d 02:31 ago)
   Statistics last cleared: Never
   Traffic statistics:
   Input bytes : 0 0 bps
   Output bytes : 322891152287160 9627472888 bps
   Input packets: 0 0 pps
   Output packets: 328809727380 1225492 pps

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Transmit-Only)

user@host> show interfaces xe-7/0/0–tx extensive

Physical interface: xe-7/0/0-tx, Enabled, Physical link is Up
   Interface index: 176, SNMP ifIndex: 137, Generation: 177
   Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
   Unidirectional: Tx-Only
   Device flags   : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Link flags     : None
   CoS queues     : 8 supported, 8 maximum usable queues
   Hold-times     : Up 0 ms, Down 0 ms
   Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
   Last flapped   : 2007-06-01 09:08:19 PDT (3d 02:31 ago)
   Statistics last cleared: Never
   Traffic statistics:
   Input bytes : 0 0 bps
   Output bytes : 322891152287160 9627472888 bps
   Input packets: 0 0 pps
   Output packets: 328809727380 1225492 pps

Filter statistics:
   Output packet count 328810554250
Logical interface xe-7/0/0-tx.0 (Index 73) (SNMP ifIndex 138) (Generation 139)

Flags: SNMP-Traps Encapsulation: ENET2
Egress account overhead: 100
Ingress account overhead: 90
Traffic statistics:
  Input bytes: 0
  Output bytes: 322891152287160
  Input packets: 0
  Output packets: 328809727380
IPv6 transit statistics:
  Input bytes: 0
  Output bytes: 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes: 0
  Output bytes: 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes: 0 0 bps
  Output bytes: 322891152287160 9627472888 bps
  Input packets: 0 0 fps
  Output packets: 328809727380 1225492 pps
IPv6 transit statistics:
  Input bytes: 0
  Output bytes: 0
  Input packets: 0
  Output packets: 0
Protocol inet, MTU: 1500, Generation: 147, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.11.12/24, Local: 10.11.12.13, Broadcast: 10.11.12.255,
  Generation: 141
Protocol multiservice, MTU: Unlimited, Generation: 148, Route table: 0
  Flags: None
  Policer: Input: __default_arp_policer__

show interfaces extensive (10-Gigabit Ethernet, LAN PHY Mode, Unidirectional Mode, Receive-Only)

user@host> show interfaces xe-7/0/0-rx extensive

Physical interface: xe-7/0/0-rx, Enabled, Physical link is Up
  Interface index: 174, SNMP ifIndex: 118, Generation: 175
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps,
  Unidirectional: Rx-Only
  Device flags: Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags: None
  CoS queues: 8 supported, 8 maximum usable queues
  Hold-times: Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:83, Hardware address: 00:00:5e:00:53:83
  Last flapped: 2007-06-01 09:08:22 PDT (3d 02:31 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes: 322857456303482 9627496104 bps

Interfaces Fundamentals for Routing Devices

Sample Output

Sample Output SRX Gigabit Ethernet

```bash
user@host> show interfaces ge-0/0/1
Physical interface: ge-0/0/1, Enabled, Physical link is Down
   Interface index: 135, SNMP ifIndex: 510
   Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
   BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
```

```bash
Output bytes : 0                  0 bps
Input packets: 328775413751       1225495 pps
Output packets: 0                   0 pps

Filter statistics:
   Input packet count 328775015056
   Input packet rejects 1
   Input DA rejects 0

Logical interface xe-7/0/0-rx.0 (Index 72) (SNMP ifIndex 120) (Generation 138)
   Flags: SNMP-Traps Encapsulation: ENET2
   Traffic statistics:
      Input bytes : 322857456303482
      Output bytes : 0
      Input packets: 328775413751
      Output packets: 0
   IPv6 transit statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Local statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Transit statistics:
      Input bytes : 322857456303482      9627496104 bps
      Output bytes : 0                  0 bps
      Input packets: 328775413751        1225495 pps
      Output packets: 0                   0 pps
   IPv6 transit statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Protocol inet, MTU: 1500, Generation: 145, Route table: 0
      Addresses, Flags: Is-Preferred Is-Primary
      Destination: 192.0.2/24, Local: 192.0.2.1, Broadcast: 192.0.2.255,
      Generation: 139
   Protocol multiservice, MTU: Unlimited, Generation: 146, Route table: 0
      Flags: None
   Policer: Input: __default_arp_policer__
```
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:42 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
Active alarms : LINK
Active defects : LINK
Interface transmit statistics: Disabled
Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514)
  Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
  Input packets : 0
  Output packets: 0
  Security: Zone: public
  Protocol inet, MTU: 1500
    Flags: Sendbcast-pkt-to-re
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255

Sample Output SRX Gigabit Ethernet

user@host> show interfaces ge-0/0/1

Physical interface: ge-0/0/1, Enabled, Physical link is Down
  Interface index: 135, SNMP ifIndex: 510
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Device flags : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
  Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:42 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  Active alarms : LINK
  Active defects : LINK
  Interface transmit statistics: Disabled
Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514)
  Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
  Input packets : 0
  Output packets: 0
  Security: Zone: public
  Protocol inet, MTU: 1500
  Flags: Sendbcast-pkt-to-re
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 1.1.1/24, Local: 1.1.1.1, Broadcast: 1.1.1.255
show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/0

Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 510
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Link-mode: Half-duplex,
  Speed: 1000mbps, BPDU Error: None, Loop Detect PDU Error: None, Ethernet-Switching
  Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
  Auto-negotiation: Enabled, Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:ef:25, Hardware address: 00:50:56:93:ef:25
  Link flags     : None
  Input rate     : 1120 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/2

Physical interface: ge-0/0/2, Enabled, Physical link is Up
  Interface index: 137, SNMP ifIndex: 525
  Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:30:40, Hardware address: 00:50:56:93:30:40

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/3

Physical interface: ge-0/0/3, Enabled, Physical link is Up
  Interface index: 138, SNMP ifIndex: 526
  Link-level type: Ethernet, MTU: 1514, Speed: 40Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 00:50:56:93:30:4d, Hardware address: 00:50:56:93:30:4d

show interfaces (Gigabit Ethernet for vSRX and vSRX 3.0)

user@host> show interfaces ge-0/0/4

Physical interface: ge-0/0/4, Enabled, Physical link is Up
  Interface index: 139, SNMP ifIndex: 527
  Link-level type: Ethernet, MTU: 1514, Speed: 100Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Ethernet-Switching Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
show interfaces detail (Gigabit Ethernet)

user@host> show interfaces ge-0/0/1 detail

Physical interface: ge-0/0/1, Enabled, Physical link is Down

Interface index: 135, SNMP ifIndex: 510, Generation: 138
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w2d 00:00 ago)
Statistics last cleared: Never
Traffic statistics:
Input  bytes :                    0                    0 bps
Output bytes :                    0                    0 bps
Input  packets:                    0                    0 pps
Output packets:                    0                    0 pps
Egress queues: 8 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets
0 best-effort                    0                    0                    0
1 expedited-fo                   0                    0                    0
2 assured-forw                   0                    0                    0
3 network-cont                   0                    0                    0
Queue number:         Mapped forwarding classes
0                   best-effort
1                   expedited-forwarding
2                   assured-forwarding
3                   network-control
Active alarms  : LINK
Active defects : LINK
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input  bytes :                    0
Output bytes :                    0
Input  packets:                    0
Output packets:                    0
Local statistics:
Input  bytes :                    0
Output bytes :                    0
Input  packets:                    0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes: 0  121859888 bps
Output bytes: 0  128104112 bps
Input packets: 0  331141 pps
Output packets: 0  348108 pps

Security: Zone: untrust
Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp ldp msdp nhrp ospf ospf3 pgm pim rip ripng router-discovery rsip sap vrrp
Flow Statistics:
Flow Input statistics:
  Self packets: 0
  ICMP packets: 0
  VPN packets: 0
  Multicast packets: 0
  Bytes permitted by policy: 525984295844
  Connections established: 7
Flow Output statistics:
  Multicast packets: 0
  Bytes permitted by policy: 576003290222
Flow error statistics (Packets dropped due to):
  Address spoofing: 0
  Authentication failed: 0
  Incoming NAT errors: 0
  Invalid zone received packet: 0
  Multiple user authentications: 0
  Multiple incoming NAT: 0
  No parent for a gate: 0
  No one interested in self packets: 0
  No minor session: 0
  No more sessions: 0
  No NAT gate: 0
  No route present: 2000280
  No SA for incoming SPI: 0
  No tunnel found: 0
  No session for a gate: 0
  No zone or NULL zone binding: 0
  Policy denied: 0
  Security association not active: 0
  TCP sequence number out of window: 0
  Syn-attack protection: 0
  User authentication errors: 0
Protocol inet, MTU: 9192
Max nh cache: 0, New hold nh limit: 0, Curr nh cnt: 0, Curr new hold cnt: 0, NH drop cnt: 0
Generation: 155, Route table: 0
Flags: Sendbcast-pkt-to-re

show interfaces extensive (Gigabit Ethernet)

user@host> show interfaces ge-0/0/1.0 extensive

Physical interface: ge-0/0/1, Enabled, Physical link is Down
Interface index: 135, SNMP ifIndex: 510, Generation: 138
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 1000mbps,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Device flags : Present Running Down
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:01, Hardware address: 00:00:5e:00:53:01
Last flapped : 2015-05-12 08:36:59 UTC (1w1d 22:57 ago)
Statistics last cleared: Never
Traffic statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pps</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
| Traffic errors:
| Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
| Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:
<table>
<thead>
<tr>
<th>Queue number</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Queue number: Mapped forwarding classes
| 0 best-effort
| 1 expedited-forwarding
| 2 assured-forwarding
| 3 network-control
Active alarms : LINK
Active defects : LINK
MAC statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Filter statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet count</td>
<td>0</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>0</td>
</tr>
<tr>
<td>CoS queues</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
</tbody>
</table>
Input SA rejects | 0
Output packet count | 0
Output packet pad count | 0
Output packet error count | 0
CAM destination filters: 2, CAM source filters: 0
Autonegotiation information:
   Negotiation status: Incomplete
Packet Forwarding Engine configuration:
   Destination slot: 0
CoS information:
   Direction : Output
   CoS transmit queue  Bandwidth  Buffer Priority
   Limit          %     bps  %     usec  Priority
   0 best-effort  95  950000000  95  0  low
   none
   3 network-control  5  50000000  5  0  low
   none
Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 514) (Generation 136)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
   Input bytes : 0
   Output bytes : 0
   Input packets: 0
   Output packets: 0
Local statistics:
   Input bytes : 0
   Output bytes : 0
   Input packets: 0
   Output packets: 0
Transit statistics:
   Input bytes : 0 0 bps
   Output bytes : 0 0 bps
   Input packets: 0 0 pps
   Output packets: 0 0 pps
Security: Zone: public
Flow Statistics:
Flow Input statistics:
   Self packets : 0
   ICMP packets : 0
   VPN packets : 0
   Multicast packets : 0
   Bytes permitted by policy : 0
   Connections established : 0
Flow Output statistics:
   Multicast packets : 0
   Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
   Address spoofing: 0
   Authentication failed: 0
   Incoming NAT errors: 0
   Invalid zone received packet: 0
   Multiple user authentications: 0
   Multiple incoming NAT: 0
   No parent for a gate: 0
   No one interested in self packets: 0
   No minor session: 0
   No more sessions: 0
show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.209.4.61/18</td>
<td></td>
</tr>
<tr>
<td>gr-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>st0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>st0.1</td>
<td>up</td>
<td>ready</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ls-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lt-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mt-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pd-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pe-0/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e3-1/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>t3-2/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>el1-3/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>se-4/0/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tl-1/5/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>br-6/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dc-6/0/0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dc-6/0/0.32767</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bc-6/0/0:1</td>
<td>down</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bc-6/0/0:1.0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dl0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dl0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dsc</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gre</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipip</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0.16385</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1</td>
<td>--&gt; 0/0</td>
</tr>
<tr>
<td>lsi</td>
<td>up</td>
<td>up</td>
<td></td>
<td>10.0.0.16</td>
<td>--&gt; 0/0</td>
</tr>
<tr>
<td>mtun</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pimd</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pime</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ppo</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show interfaces terse (vSRX and vSRX 3.0)

```
user@host> show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>up</td>
<td>up</td>
<td>INET</td>
<td>1.1.65.1/24</td>
</tr>
</tbody>
</table>
```

show interfaces controller (Channelized E1 IQ with Logical E1)

```
user@host> show interfaces controller ce1-1/2/6

<table>
<thead>
<tr>
<th>Controller</th>
<th>Admin Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce1-1/2/6</td>
<td>up</td>
</tr>
<tr>
<td>e1-1/2/6</td>
<td>up</td>
</tr>
</tbody>
</table>
```

show interfaces controller (Channelized E1 IQ with Logical DS0)

```
user@host> show interfaces controller ce1-1/2/3

<table>
<thead>
<tr>
<th>Controller</th>
<th>Admin Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>ce1-1/2/3</td>
<td>up</td>
</tr>
<tr>
<td>ds-1/2/3:1</td>
<td>up</td>
</tr>
<tr>
<td>ds-1/2/3:2</td>
<td>up</td>
</tr>
</tbody>
</table>
```

show interfaces descriptions

```
user@host> show interfaces descriptions

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-1/0/0</td>
<td>up</td>
<td>M20-3#1</td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>up</td>
<td>GSR-12#1</td>
</tr>
<tr>
<td>ge-3/0/0</td>
<td>up</td>
<td>SMB-OSPF_Area300</td>
</tr>
<tr>
<td>so-3/3/0</td>
<td>up</td>
<td>GSR-13#1</td>
</tr>
<tr>
<td>so-3/3/1</td>
<td>up</td>
<td>GSR-13#2</td>
</tr>
<tr>
<td>ge-4/0/0</td>
<td>up</td>
<td>T320-7#1</td>
</tr>
<tr>
<td>ge-5/0/0</td>
<td>up</td>
<td>T320-7#2</td>
</tr>
<tr>
<td>so-7/1/0</td>
<td>up</td>
<td>M160-6#1</td>
</tr>
<tr>
<td>ge-8/0/0</td>
<td>up</td>
<td>T320-7#3</td>
</tr>
<tr>
<td>ge-9/0/0</td>
<td>up</td>
<td>T320-7#4</td>
</tr>
<tr>
<td>so-10/0/0</td>
<td>up</td>
<td>M160-6#2</td>
</tr>
<tr>
<td>so-13/0/0</td>
<td>up</td>
<td>M20-3#2</td>
</tr>
<tr>
<td>so-14/0/0</td>
<td>up</td>
<td>GSR-12#2</td>
</tr>
<tr>
<td>ge-15/0/0</td>
<td>up</td>
<td>SMB-OSPF_Area100</td>
</tr>
<tr>
<td>ge-15/0/1</td>
<td>up</td>
<td>GSR-13#3</td>
</tr>
</tbody>
</table>
```

show interfaces destination-class all

```
user@host> show interfaces destination-class all
```
Logical interface so-4/0/0.0

<table>
<thead>
<tr>
<th>Destination class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface so-0/1/3.0

<table>
<thead>
<tr>
<th>Destination class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show interfaces diagnostics optics

user@host> show interfaces diagnostics optics ge-2/0/0

Physical interface: ge-2/0/0

- Laser bias current: 7.408 mA
- Laser output power: 0.3500 mW / -4.56 dBm
- Module temperature: 23 degrees C / 73 degrees F
- Module voltage: 3.3450 V
- Receiver signal average optical power: 0.0002 mW / -36.99 dBm
- Laser bias current high alarm: Off
- Laser bias current low alarm: Off
- Laser bias current high warning: Off
- Laser bias current low warning: Off
- Laser output power high alarm: Off
- Laser output power low alarm: Off
- Laser output power high warning: Off
- Laser output power low warning: Off
- Module temperature high alarm: Off
- Module temperature low alarm: Off
- Module temperature high warning: Off
- Module temperature low warning: Off
- Module voltage high alarm: Off
- Module voltage low alarm: Off
- Module voltage high warning: Off
- Module voltage low warning: Off
- Laser rx power high alarm: Off
- Laser rx power low alarm: Off
- Laser rx power high warning: Off
- Laser rx power low warning: Off
- Laser bias current high alarm threshold: 17.000 mA
- Laser bias current low alarm threshold: 1.000 mA
- Laser bias current high warning threshold: 14.000 mA
- Laser bias current low warning threshold: 2.000 mA
- Laser output power high alarm threshold: 0.6310 mW / -2.00 dBm
- Laser output power low alarm threshold: 0.0670 mW / -11.74 dBm
- Laser output power high warning threshold: 0.6310 mW / -2.00 dBm
- Laser output power low warning threshold: 0.0790 mW / -11.02 dBm
- Module temperature high alarm threshold: 95 degrees C / 203 degrees F
- Module temperature low alarm threshold: -25 degrees C / -13 degrees F
- Module temperature high warning threshold: 90 degrees C / 194 degrees F
- Module temperature low warning threshold: -20 degrees C / -4 degrees F
- Module voltage high alarm threshold: 3.900 V
- Module voltage low alarm threshold: 2.700 V
- Module voltage high warning threshold: 3.700 V
Module voltage low warning threshold : 2.900 V
Laser rx power high alarm threshold : 1.2590 mW / 1.00 dBm
Laser rx power low alarm threshold : 0.0100 mW / -20.00 dBm
Laser rx power high warning threshold : 0.7940 mW / -1.00 dBm
Laser rx power low warning threshold : 0.0158 mW / -18.01 dBm

show interfaces far-end-interval coc12-5/2/0

user@host> show interfaces far-end-interval coc12-5/2/0

Physical interface: coc12-5/2/0, SNMP ifIndex: 121
05:30-current:
ES-L: 1, SES-L: 1, UAS-L: 0
05:15-05:30:
ES-L: 0, SES-L: 0, UAS-L: 0
05:00-05:15:
ES-L: 0, SES-L: 0, UAS-L: 0
04:45-05:00:
ES-L: 0, SES-L: 0, UAS-L: 0
04:30-04:45:
ES-L: 0, SES-L: 0, UAS-L: 0
04:15-04:30:
ES-L: 0, SES-L: 0, UAS-L: 0
04:00-04:15:

show interfaces far-end-interval coc1-5/2/1:

user@host> run show interfaces far-end-interval coc1-5/2/1:

Physical interface: coc1-5/2/1, SNMP ifIndex: 342
05:30-current:
ES-L: 1, SES-L: 1, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
05:15-05:30:
ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
05:00-05:15:
ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:45-05:00:
ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:30-04:45:
ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:15-04:30:
ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0
04:00-04:15:

show interfaces filters

user@host> show interfaces filters

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Link Proto</th>
<th>Input Filter</th>
<th>Output Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iso</td>
<td></td>
</tr>
<tr>
<td>ge-5/0/0</td>
<td>up</td>
<td>up</td>
<td>any</td>
<td>f-any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>inet</td>
<td>f-inet</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>multservice</td>
<td></td>
</tr>
<tr>
<td>gr-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show interfaces flow-statistics (Gigabit Ethernet)

Logical interface ge-0/0/1.0 (Index 70) (SNMP ifindex 49)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 5161
  Output packets: 83
  Security: Zone: zone2
  Allowed host-inbound traffic : bootp bfd bgp dns dvmrp ldp msdp nhrp ospf
  pgm pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp ident-reset http
  https ike
  netconf ping rlogin rpm rsh snmp snmp-trap ssh telnet traceroute xnm-clear-text
  xnm-ssl
  1sging
  Flow Statistics :
  Flow Input statistics :
    Self packets :                     0
    ICMP packets :                     0
    VPN packets :                      2564
    Bytes permitted by policy :        3478
    Connections established :          1
  Flow Output statistics:
    Multicast packets :                0
    Bytes permitted by policy :        16994
  Flow error statistics (Packets dropped due to):
    Address spoofing:                  0
    Authentication failed:             0
    Incoming NAT errors:               0
    Invalid zone received packet:      0
    Multiple user authentications:     0
    Multiple incoming NAT:             0
    No parent for a gate:              0
    No one interested in self packets: 0
    No minor session:                  0
    No more sessions:                  0
    No NAT gate:                       0
    No route present:                  0
    No SA for incoming SPI:            0
    No tunnel found:                   0
    No session for a gate:             0
    No zone or NULL zone binding       0
    Policy denied:                     0
    Security association not active:   0
    TCP sequence number out of window: 0
    Syn-attack protection:            0
show interfaces interval (Channelized OC12)

user@host> show interfaces interval t3-0/3/0:0

Physical interface: t3-0/3/0:0, SNMP ifIndex: 23

17:43-current:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:28-17:43:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:13-17:28:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:58-17:13:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:43-16:58:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
...
Interval Total:
  LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,

show interfaces interval (E3)

user@host> show interfaces interval e3-0/3/0

Physical interface: e3-0/3/0, SNMP ifIndex: 23

17:43-current:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:28-17:43:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
17:13-17:28:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:58-17:13:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
  SEFS: 0, UAS: 0
16:43-16:58:
  LCV: 0, PCV: 0, CCV: 0, LES: 0, PES: 0, PSES: 0, CES: 0, CSES: 0,
...
Interval Total:
  LCV: 230, PCV: 1145859, CCV: 455470, LES: 0, PES: 230, PSES: 230,

show interfaces interval (SONET/SDH) (SRX devices)

user@host> show interfaces interval so-0/1/0
Physical interface: so-0/1/0, SNMP ifIndex: 19

20:02-current:
  ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0

19:47-20:02:

19:32-19:47:

19:17-19:32:
  ES-S: 0, SES-S: 0, SEFS-S: 0, ES-L: 0, SES-L: 0, UAS-L: 0, ES-P: 0, SES-P: 0, UAS-P: 0

19:02-19:17:
  ....

show interfaces load-balancing (SRX devices)

user@host> show interfaces load-balancing

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Member count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams0</td>
<td>Up</td>
<td>1d 00:50</td>
<td>2</td>
</tr>
<tr>
<td>ams1</td>
<td>Up</td>
<td>00:00:59</td>
<td>2</td>
</tr>
</tbody>
</table>

show interfaces load-balancing detail (SRX devices)

user@host> show interfaces load-balancing detail

Load-balancing interfaces detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Member count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams0</td>
<td>Up</td>
<td>1d 00:51</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Members</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Weight</td>
<td>State</td>
<td></td>
</tr>
<tr>
<td>mams-2/0/0</td>
<td>10</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>mams-2/1/0</td>
<td>10</td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

show interfaces mac-database (All MAC Addresses on a Port SRX devices)

user@host> show interfaces mac-database xe-0/3/3

Physical interface: xe-0/3/3, Enabled, Physical link is Up

Interface index: 372, SNMP ifIndex: 788

Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, Loopback: None, Source filtering: Disabled, Flow control: Enabled

Device flags : Present Running

Interface flags: SNMP-Traps Internal: 0x4000

Link flags : None

Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)

Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2

<table>
<thead>
<tr>
<th>MAC address</th>
<th>Input frames</th>
<th>Input bytes</th>
<th>Output frames</th>
<th>Output bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:00:00</td>
<td>1</td>
<td>56</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00:00:01:01:01:02</td>
<td>7023810</td>
<td>323095260</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00:00:01:01:01:03</td>
<td>7023810</td>
<td>323095260</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>00:00:00:01:01:01:04</td>
<td>7023810</td>
<td>323095260</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces mac-database (All MAC Addresses on a Service SRX devices)

user@host> show interfaces mac-database xe-0/3/3

Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2

MAC address    Input frames    Input bytes  Output frames   Output bytes
00:00:00:00:00:00             1             56              0              0
00:00:c0:01:01:02       7023810      323095260              0              0
00:00:c0:01:01:03       7023810      323095260              0              0
00:00:c0:01:01:04       7023810      323095260              0              0
00:00:c0:01:01:05       7023810      323095260              0              0
00:00:c0:01:01:06       7023810      323095260              0              0
00:00:c0:01:01:07       7023810      323095260              0              0
00:00:c0:01:01:08       7023809      323095214              0              0
00:00:c0:01:01:09       7023809      323095214              0              0
00:00:c0:01:01:0a       7023809      323095214              0              0
00:00:c0:01:01:0b       7023809      323095214              0              0
00:00:c8:01:01:02      30424784     1399540064       37448598     1722635508
00:00:c8:01:01:03      30424784     1399540064       37448598     1722635508
00:00:c8:01:01:04      30424716     1399536936       37448523     1722632058
00:00:c8:01:01:05      30424789     1399540294       37448598     1722635508
00:00:c8:01:01:06      30424788     1399540248       37448597     1722635462
00:00:c8:01:01:07      30424783     1399540018       37448597     1722635462
00:00:c8:01:01:08      30424783     1399540018       37448596     1722635416
00:00:c8:01:01:09       8836796      406492616        8836795      406492570
00:00:c8:01:01:0a      30424712     1399536752       37448521     1722631966
00:00:c8:01:01:0b      30424715     1399536890       37448523     1722632058

Number of MAC addresses : 21

show interfaces mac-database mac-address

user@host> show interfaces mac-database xe-0/3/3 mac-address

Logical interface xe-0/3/3 (Index 364) (SNMP ifIndex 829)
Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2

MAC address    Input frames    Input bytes  Output frames   Output bytes
00:00:00:00:00:00             1             56              0              0
00:00:c0:01:01:02       7023810      323095260              0              0
00:00:c0:01:01:03       7023810      323095260              0              0
00:00:c0:01:01:04       7023810      323095260              0              0
00:00:c0:01:01:05       7023810      323095260              0              0
00:00:c0:01:01:06       7023810      323095260              0              0
00:00:c0:01:01:07       7023810      323095260              0              0
00:00:c0:01:01:08       7023809      323095214              0              0
00:00:c0:01:01:09       7023809      323095214              0              0
00:00:c0:01:01:0a       7023809      323095214              0              0
00:00:c0:01:01:0b       7023809      323095214              0              0
00:00:c8:01:01:02      30424784     1399540064       37448598     1722635508
00:00:c8:01:01:03      30424784     1399540064       37448598     1722635508
00:00:c8:01:01:04      30424716     1399536936       37448523     1722632058
00:00:c8:01:01:05      30424789     1399540294       37448598     1722635508
00:00:c8:01:01:06      30424788     1399540248       37448597     1722635462
00:00:c8:01:01:07      30424783     1399540018       37448597     1722635462
00:00:c8:01:01:08      30424783     1399540018       37448596     1722635416
00:00:c8:01:01:09       8836796      406492616        8836795      406492570
00:00:c8:01:01:0a      30424712     1399536752       37448521     1722631966
00:00:c8:01:01:0b      30424715     1399536890       37448523     1722632058

Physical interface: xe-0/3/3, Enabled, Physical link is Up
Interface index: 372, SNMP ifIndex: 788
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, Loopback: None, Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running

Chapter 14: Interface Operational Commands
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None

Logical interface xe-0/3/3.0 (Index 364) (SNMP ifIndex 829)
Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
MAC address: 00:00:c8:01:01:09, Type: Configured,
Input bytes : 202324652
Output bytes : 202324560
Input frames : 4398362
Output frames : 4398360
Policer statistics:
Policer type Discarded frames Discarded bytes
Output aggregate 3992386 183649756

show interfaces mc-ae (SRX devices)

user@host> show interfaces mc-ae ae0 unit 512
Member Links : ae0
Local Status : active
Peer Status : active
Logical Interface : ae0.512
Core Facing Interface : Label Ethernet Interface
ICL-PL : Label Ethernet Interface

show interfaces media (SONET/SDH)

The following example displays the output fields unique to the `show interfaces media` command for a SONET interface (with no level of output specified):

user@host> show interfaces media so-4/1/2
Physical interface: so-4/1/2, Enabled, Physical link is Up
Interface index: 168, SNMP ifIndex: 495
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps 16384
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 1783 (00:00:00 ago), Output: 1786 (00:00:08 ago)
LCP state: Opened
CHAP state: Not-configured
CoS queues : 8 supported
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : None
SONET defects : None
SONET errors:
  BIP-B1: 1, BIP-B2: 2, BIP-B3: 3, BIP-B4: 4, BIP-BIP2: 0
Received path trace: routerb so-1/1/2
Transmitted path trace: routera so-4/1/2
show interfaces policers (SRX devices)

```
user@host> show interfaces policers

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Proto</th>
<th>Input Policer</th>
<th>Output Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iso</td>
<td></td>
</tr>
<tr>
<td>gr-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mt-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pd-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pe-0/3/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>so-2/0/0.0-in-policer so-2/0/0.0-out-policer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iso</td>
<td></td>
</tr>
<tr>
<td>so-2/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

show interfaces policers interface-name (SRX devices)

```
user@host> show interfaces policers so-2/1/0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Link</th>
<th>Proto</th>
<th>Input Policer</th>
<th>Output Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-2/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/1/0.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>so-2/1/0.0-in-policer so-2/1/0.0-out-policer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>iso</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>inet6</td>
<td></td>
</tr>
</tbody>
</table>
```

show interfaces queue (SRX devices)

```
The following truncated example shows the CoS queue sizes for queues 0, 1, and 3. Queue 1 has a queue buffer size (guaranteed allocated memory) of 9192 bytes.

user@host> show interfaces queue

Physical interface: ge-0/0/0, Enabled, Physical link is Up
Interface index: 134, SNMP ifIndex: 509
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: class0
Queued:
  Packets       : 0       0 pps
  Bytes         : 0       0 bps
Transmitted:
  Packets       : 0       0 pps
  Bytes         : 0       0 bps
  Tail-dropped packets : 0       0 bps
  RL-dropped packets : 0       0 bps
  RL-dropped bytes : 0       0 bps
  RED-dropped packets : 0       0 bps
  Low            : 0       0 pps
  Medium-low     : 0       0 pps
  Medium-high    : 0       0 pps
  High           : 0       0 pps
  RED-dropped bytes : 0       0 bps
  Low            : 0       0 bps
```
show interfaces redundancy (SRX devices)

user@host> show interfaces redundancy

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Primary</th>
<th>Secondary</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsp0</td>
<td>Not present</td>
<td></td>
<td></td>
<td></td>
<td>both down</td>
</tr>
<tr>
<td>rsp1</td>
<td>On secondary</td>
<td>1d 23:56</td>
<td>sp-1/0/0</td>
<td>sp-0/2/0</td>
<td>primary down</td>
</tr>
<tr>
<td>rsp2</td>
<td>On primary</td>
<td>10:10:27</td>
<td>sp-1/3/0</td>
<td>sp-0/2/0</td>
<td>secondary down</td>
</tr>
<tr>
<td>rlsq0</td>
<td>On primary</td>
<td>00:06:24</td>
<td>lsq-0/3/0</td>
<td>lsq-1/0/0</td>
<td>both up</td>
</tr>
</tbody>
</table>

show interfaces redundancy (Aggregated Ethernet SRX devices)

user@host> show interfaces redundancy

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
<th>Primary</th>
<th>Secondary</th>
<th>Current status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlsq0</td>
<td>On secondary</td>
<td>00:56:12</td>
<td>lsq-4/0/0</td>
<td>lsq-3/0/0</td>
<td>both up</td>
</tr>
</tbody>
</table>

show interfaces redundancy detail (SRX devices)

user@host> show interfaces redundancy detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Last change</th>
</tr>
</thead>
<tbody>
<tr>
<td>rlsq0</td>
<td>On primary</td>
<td>00:45:47</td>
</tr>
</tbody>
</table>
Primary: lsq-0/2/0
Secondary: lsq-1/2/0
Current status: both up
Mode: hot-standby

Interface: rlsq0:0
State: On primary
Last change: 00:45:46
Primary: lsq-0/2/0:0
Secondary: lsq-1/2/0:0
Current status: both up
Mode: warm-standby

show interfaces routing brief (SRX devices)

user@host> show interfaces routing brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-5/0/3.0</td>
<td>Down</td>
<td>ISO enabled</td>
</tr>
<tr>
<td>so-5/0/2.0</td>
<td>Up</td>
<td>MPLS enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.2.120</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>so-5/0/1.0</td>
<td>Up</td>
<td>MPLS enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.2.130</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>at-1/0/0.3</td>
<td>Up</td>
<td>CCC enabled</td>
</tr>
<tr>
<td>at-1/0/0.2</td>
<td>Up</td>
<td>CCC enabled</td>
</tr>
<tr>
<td>at-1/0/0.0</td>
<td>Up</td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 192.168.90.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET enabled</td>
</tr>
<tr>
<td>lo0.0</td>
<td>Up</td>
<td>ISO 47.0005.80ff.f800.0000.0108.0001.1921.6800.5061.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INET 127.0.0.1</td>
</tr>
<tr>
<td>fxp1.0</td>
<td>Up</td>
<td>INET 192.168.6.90</td>
</tr>
<tr>
<td>fxp0.0</td>
<td>Up</td>
<td>INET 192.168.6.90</td>
</tr>
</tbody>
</table>

show interfaces routing detail (SRX devices)

user@host> show interfaces routing detail

so-5/0/3.0
Index: 15, Refcount: 2, State: Up <Broadcast PointToPoint Multicast> Change:<>
Metric: 0, Up/down transitions: 0, Full-duplex
Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
ISO address (null)
State: <Broadcast PointToPoint Multicast> Change: <>
Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes

so-5/0/2.0
Index: 14, Refcount: 7, State: <Up Broadcast PointToPoint Multicast> Change:<>
Metric: 0, Up/down transitions: 0, Full-duplex
Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
MPLS address (null)
State: <Up Broadcast PointToPoint Multicast> Change: <>
Preference: 0 (120 down), Metric: 0, MTU: 4458 bytes
ISO address (null)
show interfaces routing-instance all (SRX devices)

user@host> show interfaces terse routing-instance all

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-0/0/1</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1/24</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>192.168.4.28/24</td>
<td>sample-a</td>
</tr>
<tr>
<td>at-0/1/0.0</td>
<td>up</td>
<td>up</td>
<td>inet6</td>
<td>fe80::a:0:0:4/64</td>
<td>sample-b</td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.1/32</td>
<td></td>
</tr>
</tbody>
</table>

show interfaces snmp-index (SRX devices)

user@host> show interfaces snmp-index 33

Physical interface: so-2/1/1, Enabled, Physical link is Down
Interface index: 149, SNMP ifIndex: 33
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps 16384
CoS queues : 8 supported
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : LOL, PLL, LOS
SONET defects : LOL, PLL, LOF, LOS, SEF, AIS-L, AIS-P

show interfaces source-class all (SRX devices)

user@host> show interfaces source-class all

Logical interface so-0/1/0.0

<table>
<thead>
<tr>
<th>Source class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>1928095</td>
<td>161959980</td>
</tr>
<tr>
<td></td>
<td>(889)</td>
<td>(597762)</td>
</tr>
<tr>
<td>bronze</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface so-0/1/3.0

<table>
<thead>
<tr>
<th>Source class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gold</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bronze</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces statistics (Fast Ethernet SRX devices)

user@host> show interfaces fe-1/3/1 statistics

Physical interface: fe-1/3/1, Enabled, Physical link is Up
Interface index: 144, SNMP ifIndex: 1042
Description: ford fe-1/3/1
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues : 4 supported, 4 maximum usable queues
Current address: 00:90:69:93:04:dc, Hardware address: 00:90:69:93:04:dc
Last flapped : 2006-04-18 03:08:59 PDT (00:01:24 ago)
Statistics last cleared: Never
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
Input errors: 0, Output errors: 0
Active alarms : None
Active defects : None
Logical interface fe-1/3/1.0 (Index 69) (SNMP ifIndex 50)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500
Flags: Is-Primary, DCU, SCU-in

<table>
<thead>
<tr>
<th>Destination class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>silver1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 10.27.245/24, Local: 10.27.245.2,
Broadcast: 10.27.245.255
Protocol iso, MTU: 1497
Flags: Is-Primary

show interfaces switch-port (SRX devices)

user@host# show interfaces ge-slot/0/0 switch-port port-number

Port 0, Physical link is Up
Speed: 100mbps, Auto-negotiation: Enabled

Statistics:

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total bytes</td>
<td>28437086</td>
<td>21792250</td>
</tr>
<tr>
<td>Total packets</td>
<td>409145</td>
<td>88008</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>9987</td>
<td>83817</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>145002</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>254156</td>
<td>4191</td>
</tr>
<tr>
<td>Multiple collisions</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td>FIFO/CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Runt frames</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Jabber frames 0
Fragment frames 0
Discarded frames 0

Autonegotiation information:
  Negotiation status: Complete
  Link partner:
    Link mode: Full-duplex, Flow control: None, Remote fault: OK, Link partner Speed: 100 Mbps
  Local resolution:
    Flow control: None, Remote fault: Link OK

show interfaces transport pm (SRX devices)

```bash
show interfaces transport pm all current et-0/1/0
```

Physical interface: et-0/1/0, SNMP ifIndex 515

<table>
<thead>
<tr>
<th>Near End PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU-BBE</td>
<td>0</td>
<td>800</td>
</tr>
<tr>
<td>OTU-ES</td>
<td>0</td>
<td>135</td>
</tr>
<tr>
<td>OTU-SES</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>OTU-UAS</td>
<td>427</td>
<td>90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Far End PM</th>
<th>Suspect Flag:True</th>
<th>Reason:Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU-BBE</td>
<td>0</td>
<td>800</td>
</tr>
<tr>
<td>OTU-ES</td>
<td>0</td>
<td>135</td>
</tr>
<tr>
<td>OTU-SES</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>OTU-UAS</td>
<td>0</td>
<td>90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Near End PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODU-BBE</td>
<td>0</td>
<td>800</td>
</tr>
<tr>
<td>ODU-ES</td>
<td>0</td>
<td>135</td>
</tr>
<tr>
<td>ODU-SES</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>ODU-UAS</td>
<td>427</td>
<td>90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Far End PM</th>
<th>Suspect Flag:True</th>
<th>Reason:Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODU-BBE</td>
<td>0</td>
<td>800</td>
</tr>
<tr>
<td>ODU-ES</td>
<td>0</td>
<td>135</td>
</tr>
<tr>
<td>ODU-SES</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>ODU-UAS</td>
<td>0</td>
<td>90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FEC PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEC-CorrectedErr</td>
<td>2008544300</td>
<td>0</td>
</tr>
<tr>
<td>FEC-UncorrectedWords</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BER PM</th>
<th>Suspect Flag:False</th>
<th>Reason:None</th>
</tr>
</thead>
<tbody>
<tr>
<td>BER</td>
<td>3.6e-5</td>
<td>5.8e-5</td>
</tr>
</tbody>
</table>

Physical interface: et-0/1/0, SNMP ifIndex 515

<table>
<thead>
<tr>
<th>Suspect Flag:True</th>
<th>Reason:Object Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>BER</td>
<td>CURRENT MIN MAX AVG THRESHOLD</td>
</tr>
<tr>
<td>TCA-ENABLED</td>
<td>TCA-RAISED</td>
</tr>
<tr>
<td></td>
<td>(MAX)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Lane chromatic dispersion</td>
<td>0</td>
</tr>
<tr>
<td>Lane differential group delay</td>
<td>0</td>
</tr>
<tr>
<td>q Value</td>
<td>120</td>
</tr>
<tr>
<td>SNR</td>
<td>28</td>
</tr>
<tr>
<td>Tx output power (0.01dBm)</td>
<td>-5000</td>
</tr>
<tr>
<td>Rx input power (0.01dBm)</td>
<td>-3642</td>
</tr>
<tr>
<td>Module temperature (Celsius)</td>
<td>46</td>
</tr>
<tr>
<td>Tx laser bias current (0.1mA)</td>
<td>0</td>
</tr>
<tr>
<td>Rx laser bias current (0.1mA)</td>
<td>1270</td>
</tr>
<tr>
<td>Carrier frequency offset (MHz)</td>
<td>-186</td>
</tr>
</tbody>
</table>

show security zones (SRX devices)

user@host> show security zones

Functional zone: management
  Description: This is the management zone.
  Policy configurable: No
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0

Security zone: Host
  Description: This is the host zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    fxp0.0

Security zone: abc
  Description: This is the abc zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0

Security zone: def
  Description: This is the def zone.
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/2.0
show interfaces (M Series, MX Series, T Series Routers, and PTX Series Management and Internal Ethernet)

**List of Syntax**

Syntax (M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface) on page 1476
Syntax (M Series, MX Series, T Series, and PTX Series Routers Internal Ethernet Interface) on page 1476

Syntax (M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface)

```plaintext
show interfaces em0 | fxp0 | mgmtre0
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>
```

Syntax (M Series, MX Series, T Series, and PTX Series Routers Internal Ethernet Interface)

```plaintext
show interfaces bcm0 | em0 | em1 | fxp1 | fxp2 | ixgbe0 | ixgbe1
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

(M Series, T Series, TX Matrix Plus, and PTX Series devices only) Display status information about the management Ethernet and internal Ethernet interfaces.

**Options**

em0 | fxp0 | mgmtre0—(M Series, MX Series, T Series, and PTX Series) Display standard information about the management Ethernet interface. For supported Ethernet interface by chassis and Routing Engine, see Supported Routing Engines by Router.

bcm0 | em0 | em1 | fxp1 | fxp2 | ixgbe0 | ixgbe1—(M Series, MX Series, T Series, and PTX Series) Display standard information about the internal Ethernet interfaces. See Supported Routing Engines by Router for the internal Ethernet interface names for each Routing Engine by hardware platform.

**NOTE:** On Junos OS Evolved, the ixgbe0 and ixgbe1 internal interfaces are deprecated.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.
**media**—(Optional) Display media-specific information.

**snmp-index**

**snmp-index**—(Optional) Display information for the specified SNMP index of the interface.

**statistics**—(Optional) Display static interface statistics.

---

**Required Privilege** view

**List of Sample Output**

```
show interfaces brief (Management Ethernet) on page 1480
show interfaces (Management Ethernet) on page 1480
show interfaces (Management Ethernet [TX Matrix Plus Router]) on page 1481
show interfaces (Management Ethernet [PTX Series Packet Transport Routers]) on page 1481
show interfaces detail (Management Ethernet) on page 1482
show interfaces detail (Management Ethernet [TX Matrix Plus Router]) on page 1482
show interfaces detail (Management Ethernet [PTX Packet Transport Routers]) on page 1483
show interfaces extensive (Management Ethernet) on page 1484
show interfaces extensive (Management Ethernet [TX Matrix Plus Router]) on page 1484
show interfaces extensive (Management Ethernet [PTX Series Packet Transport Routers]) on page 1485
show interfaces mgmtre0 (Management Ethernet [PTX5000 Router]) on page 1486
show interfaces brief (Management Ethernet) on page 1487
show interfaces brief (Management Ethernet [TX Matrix Plus Router]) on page 1487
show interfaces brief (Management Ethernet [PTX Series Packet Transport Routers]) on page 1487
show interfaces (Internal Ethernet) on page 1487
show interfaces (Internal Ethernet [TX Matrix Plus Router]) on page 1488
show interfaces detail (Internal Ethernet) on page 1489
show interfaces detail (Internal Ethernet [TX Matrix Plus Router]) on page 1489
show interfaces extensive (Internal Ethernet) on page 1490
show interfaces extensive (internal Ethernet [TX Matrix Plus Router]) on page 1491
```

---

**Output Fields**

Table 44 on page 1477 lists the output fields for the **show interfaces** (management) command on the M Series routers, T Series routers, TX Matrix Plus routers, and PTX Series. Output fields are listed in the approximate order in which they appear.

**Table 44: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</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>Interface index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation type used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU)—Size of the largest packet to be transmitted.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Network speed on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link type</td>
<td>Data transmission type.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Physical info</td>
<td>Information about the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down. Value is in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Media access control (MAC) address of the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup link address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the physical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the physical interface.</td>
<td>None specified</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>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the logical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>and physical interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes, Output bytes</strong>—Number of bytes received and transmitted on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets, Output packets</strong>—Number of packets received and transmitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Input errors</strong></td>
<td>• <strong>Errors</strong>—Input errors on the interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runts</strong>—Frames received smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Frames received larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policied Discards</strong>—Frames that the incoming packet match code discarded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>because they were not recognized or were not of interest. Usually, this field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reports protocols that Junos does not support.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>up</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly, increasing only when the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cable is unplugged, the far-end system is powered down and then up, or another</td>
<td></td>
</tr>
<tr>
<td></td>
<td>problem occurs. If the number of carrier transitions increments quickly,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>possibly once every 10 seconds, the cable, the remote system, or the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the interface is saturated, this number increments once for every packet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dropped by the ASIC RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Index</strong></td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>Logical Interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the logical interface; values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Encapsulation on the logical interface.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
### Table 44: show interfaces Output Fields for M Series, MX Series, T Series, and PTX Series Routers Management Ethernet Interface (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet</td>
<td>IP address of the logical interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface (such as iso or inet6).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Route table in which this address exists. For example, Route table:0 refers to inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the &quot;Family Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about address flags. Possible values are described in the &quot;Addresses Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

### Sample Output

**show interfaces brief (Management Ethernet)**

```plaintext
user@host> show interfaces fxlO brief
Physical interface: fxlO, Enabled, Physical link is Up
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified, Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps

Logical interface fxlO.0
Flags: SNMP-Traps Encapsulation: ENET2
inet 192.168.70.143/21
```

**show interfaces (Management Ethernet)**

```plaintext
user@host> show interfaces fxlO
Physical interface: fxlO, Enabled, Physical link is Up
Interface index: 1, SNMP ifIndex: 1
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
```
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Half-Duplex
Current address: 00:00:5E:00:53:89, Hardware address: 00:00:5E:00:53:89
Last flapped : Never
   Input packets : 80804
   Output packets: 1105

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13)
   Flags: SNMP-Traps Encapsulation: ENET2
   Protocol inet, MTU: 1500
   Flags: Is-Primary
   Addresses, Flags: Is-Preferred Is-Primary
      Destination: 192.168.64/21, Local: 192.168.70.143,
      Broadcast: 192.168.71.255

show interfaces (Management Ethernet [TX Matrix Plus Router])

user@host> show interfaces em0

Physical interface: em0, Enabled, Physical link is Up
   Interface index: 8, SNMP ifIndex: 17
   Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
   Device flags : Present Running
   Interface flags: SNMP-Traps
   Link type : Full-Duplex
   Current address: 00:00:5E:00:53:c0, Hardware address: 00:00:5E:00:53:c0
   Last flapped : Never
   Input packets : 1424
   Output packets: 5282

Logical interface em0.0 (Index 3) (SNMP ifIndex 18)
   Flags: SNMP-Traps Encapsulation: ENET2
   Input packets : 1424
   Output packets: 5282
   Protocol inet, MTU: 1500
   Flags: Is-Primary
   Addresses, Flags: Is-Preferred Is-Primary

show interfaces (Management Ethernet [PTX Series Packet Transport Routers])

user@host> show interfaces em0

Physical interface: em0, Enabled, Physical link is Up
   Interface index: 8, SNMP ifIndex: 0
   Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
   Device flags : Present Running
   Interface flags: SNMP-Traps
   Link type : Full-Duplex
   Current address: 00:00:5E:00:53:1b, Hardware address: 00:00:5E:00:53:1b
   Last flapped : Never
   Input packets : 212581
   Output packets: 71

   Logical interface em0.0 (Index 3) (SNMP ifIndex 0)
   Flags: SNMP-Traps Encapsulation: ENET2
   Input packets : 212551
Output packets: 71
Protocol inet, MTU: 1500
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 192.168.3/24, Local: 192.168.3.30,
Broadcast: 192.168.3.255

show interfaces detail (Management Ethernet)

user@host> show interfaces fxp0 detail

Physical interface: fxp0, Enabled, Physical link is Up
Interface index: 1, SNMP ifIndex: 1, Generation: 0
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Half-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:89, Hardware address: 00:00:5E:00:53:89
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input  bytes  :              6484031
Output bytes  :               167503
Input  packets:                81008
Output packets:                 1110

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13) (Generation 1)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 6, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred Is-Primary
Destination: 192.168.64/21, Local: 192.168.70.143,
Broadcast: 192.168.71.255, Generation: 1

show interfaces detail (Management Ethernet [TX Matrix Plus Router])

user@host> show interfaces em0 detail

Physical interface: em0, Enabled, Physical link is Up
Interface index: 8, SNMP ifIndex: 17, Generation: 2
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:c0, Hardware address: 00:00:5E:00:53:c0
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input  bytes  :               124351
Output bytes  :              1353212
Input  packets:                 1804

Copyright © 2019, Juniper Networks, Inc.
show interfaces detail (Management Ethernet [PTX Packet Transport Routers])

user@host> show interfaces detail em0

Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0, Generation: 3
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
    Speed: 1000mbps
  Device flags   : Present Running
  Interface flags: SNMP-Traps
  Link type      : Full-Duplex
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:00:5E:00:53:1b, Hardware address: 00:00:5E:00:53:1b
  Alternate link address: Unspecified
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
  Input bytes : 15255909
  Output bytes : 4608
  Input packets: 214753
  Output packets: 72
  IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0

Logical interface em0.0 (Index 3) (SNMP ifIndex 18) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
  Input bytes : 117135
  Output bytes : 1331647
  Input packets: 1804
  Output packets: 5344
  Local statistics:
  Input bytes : 117135
  Output bytes : 1331647
  Input packets: 1804
  Output packets: 5344
  Protocol inet, MTU: 1500, Generation: 1, Route table: 0
    Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 192.168.178.0/25, Local: 192.168.178.11, Broadcast:
      192.168.178.127, Generation: 1
Output packets: 72
Local statistics:
Input bytes: 14394630
Output bytes: 3024
Input packets: 214723
Output packets: 72
Protocol inet, MTU: 1500, Generation: 1, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
  Destination: 192.168.3/24, Local: 192.168.3.30,
  Broadcast: 192.168.3.255, Generation: 1

show interfaces extensive (Management Ethernet)

user@host> show interfaces fxp0 extensive

Physical interface: fxp0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 1, Generation: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags: Present Running
  Interface flags: SNMP-Traps
  Link type: Half-Duplex
  Physical info: Unspecified
  Hold-times: Up 0 ms, Down 0 ms
  Current address: 00:00:5E:00:53:89, Hardware address: 00:00:5E:00:53:89
  Alternate link address: Unspecified
  Last flapped: Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes: 6678904
    Output bytes: 169657
    Input packets: 83946
    Output packets: 1127
  Input errors:
    Errors: 12, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0

Logical interface fxp0.0 (Index 2) (SNMP ifIndex 13) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Protocol inet, MTU: 1500, Generation: 6, Route table: 0
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 192.168.64/21, Local: 192.168.70.143,
    Broadcast: 192.168.71.255, Generation: 1

show interfaces extensive (Management Ethernet [TX Matrix Plus Router])

user@host> show interfaces em0 extensive

Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 17, Generation: 2
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 100mbps
  Device flags: Present Running
show interfaces extensive (Management Ethernet [PTX Series Packet Transport Routers])

user@host> show interfaces extensive em0

Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0, Generation: 3
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Physical info : Unspecified
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:00:5E:00:53:1b, Hardware address: 00:00:5E:00:53:1b
  Alternate link address: Unspecified
  Last flapped : Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 119748
    Output bytes: 1335719
    Input packets: 1843
    Output packets: 5372
  Protocol inet, MTU: 1500, Generation: 1, Route table: 0
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred Is-Primary
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 15236459
  Output bytes : 4608
  Input packets: 214482
  Output packets: 72
IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0

Logical interface em0.0 (Index 3) (SNMP ifIndex 0) (Generation 1)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes : 14376264
    Output bytes : 3024
    Input packets: 214452
    Output packets: 72
  Local statistics:
    Input bytes : 14376264
    Output bytes : 3024
    Input packets: 214452
    Output packets: 72
  Protocol inet, MTU: 1500, Generation: 1, Route table: 0
    Flags: Is-Primary
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 192.168.3/24, Local: 192.168.3.30,
    Broadcast: 192.168.3.255, Generation: 1

show interfaces mgmtre0 (Management Ethernet [PTX5000 Router])
user@host> show interfaces mgmtre0 extensive
Physical interface: mgmtre0, Enabled, Physical link is Up
  Interface index: 1001, SNMP ifIndex: 501
  Link-level type: Ethernet, MTU: 1500
  Device flags : Present
  Interface flags : None
  Link flags : None
  Current address: ec:9e:cd:06:30:da, Hardware address: ec:9e:cd:06:30:da
  Last flapped : Never

Logical interface mgmtre0.0 (Index 1001) (SNMP ifIndex 503)
  Flags: Encapsulation: ENET2
  Protocol inet, MTU: 1486
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.92.248/23, Local: 10.92.248.22,
    Broadcast: 10.92.249.255
  Protocol multiservice, MTU: Unlimited
    Flags: None
show interfaces brief (Management Ethernet)

user@host> show interfaces fxp1 brief

Physical interface: fxp1, Enabled, Physical link is Up
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps

Logical interface fxp1.0
Flags: SNMP-Traps Encapsulation: ENET2
inet 10.0.0.4/8
inet6 fe80::200:ff:fe00:4/64
    fec0::10:0:0:4/64
tnp 4

show interfaces brief (Management Ethernet [TX Matrix Plus Router])

user@host> show interfaces em0 brief

Physical interface: em0, Enabled, Physical link is Up
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps

Logical interface em0.0
Flags: SNMP-Traps Encapsulation: ENET2
inet 192.168.178.11/25

show interfaces brief (Management Ethernet [PTX Series Packet Transport Routers])

user@host> show interfaces em0 brief

Physical interface: em0, Enabled, Physical link is Up
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
Speed: 1000mbps
Device flags : Present Running
Interface flags: SNMP-Traps

Logical interface em0.0
Flags: SNMP-Traps Encapsulation: ENET2
inet 192.168.3.30/24

root@aboslutely> show interfaces em0 terse
Interface               Admin Link Proto    Local                 Remote
em0                     up    up
em0.0                   up    up   inet     192.168.3.30/24

show interfaces (Internal Ethernet)

user@host> show interfaces fxp1

Physical interface: fxp1, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 2
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
show interfaces (Internal Ethernet [TX Matrix Plus Router])

Physical interface: ixgbe0, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 116
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
Device flags: Present Running
Interface flags: SNMP-Traps
Link type: Full-Duplex
Current address: 00:00:5E:00:53:04, Hardware address: 00:00:5E:00:53:04
Last flapped: Never
Input packets: 2301738
Output packets: 3951155

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117)
Flags: SNMP-Traps Encapsulation: ENET2
Input packets: 2301595
Output packets: 3951155
Protocol inet, MTU: 1500
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: 10/8, Local: 10.34.0.4, Broadcast: 10.255.255.255
Addresses, Flags: Primary Is-Default Is-Preferred Is-Primary
Destination: 192.168/16, Local: 192.168.0.4, Broadcast: 192.168.0.4
Protocol inet6, MTU: 1500
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::200:ff:fe22:4
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: fec0::/64, Local: fec0::a:22:0:4
Protocol tnp, MTU: 1500
Flags: Primary, Is-Primary
Addresses
Local: 0x22000004
show interfaces detail (Internal Ethernet)

user@host> show interfaces fxp1 detail

Physical interface: fxp1, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 2, Generation: 1
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified, Speed: 100mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:04, Hardware address: 00:00:5E:00:53:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input  bytes : 2339969
Output bytes : 15880707
Input  packets: 30758
Output packets: 33443

Logical interface fxp1.0 (Index 3) (SNMP ifIndex 14) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 7, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: 10/8, Local: 10.0.0.4, Broadcast: 10.255.255.255,
Generation: 3
Protocol inet6, MTU: 1500, Generation: 8, Route table: 1
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::200:ff:fe00:4,
Broadcast: Unspecified, Generation: 5
Addresses, Flags: Is-Default Is-Preferred Is-Primary
Destination: fec0::/64, Local: fec0::10:0:0:4, Broadcast: Unspecified,
Generation: 7
Protocol tnp, MTU: 1500, Generation: 9, Route table: 1
Flags: Primary, Is-Primary
Addresses, Flags: None
Destination: Unspecified, Local: 4, Broadcast: Unspecified,
Generation: 8

show interfaces detail (Internal Ethernet [TX Matrix Plus Router])

user@host> show interfaces ixgbe0 detail

Physical interface: ixgbe0, Enabled, Physical link is Up
Interface index: 2, SNMP ifIndex: 116, Generation: 3
Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified, Speed: 1000mbps
Device flags : Present Running
Interface flags: SNMP-Traps
Link type : Full-Duplex
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:04, Hardware address: 00:00:5E:00:53:04
Alternate link address: Unspecified
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes :        238172825
  Output bytes :       1338948955
  Input packets:       2360984
  Output packets:      4061512
IPv6 transit statistics:
  Input bytes :         0
  Output bytes :        0
  Input packets:        0
  Output packets:       0

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117) (Generation 2)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes :        228720309
    Output bytes :       1261387447
    Input packets:       2360841
    Output packets:      4061512
IPv6 transit statistics:
    Input bytes :         0
    Output bytes :        0
    Input packets:        0
    Output packets:       0
Local statistics:
  Input bytes :        228720309
  Output bytes :       1261387447
  Input packets:       2360841
  Output packets:      4061512

Protocol inet, MTU: 1500, Generation: 2, Route table: 1
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred
    Destination: 10/8, Local: 10.34.0.4, Broadcast: 10.255.255.255, Generation: 2

Protocol inet6, MTU: 1500, Generation: 3, Route table: 1
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::200:ff:fe22:4

Protocol tnp, MTU: 1500, Generation: 5
  Generation: 4, Route table: 1
  Flags: Primary, Is-Primary
  Addresses, Flags: None
    Destination: Unspecified, Local: 0x22000004, Broadcast: Unspecified, Generation: 6

Interfaces Fundamentals for Routing Devices
Interface flags: SNMP-Traps
Link type: Full-Duplex
Physical info: Unspecified
Hold-times: Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:04, Hardware address: 00:00:5E:00:53:04
Alternate link address: Unspecified
Last flapped: Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes: 2349897
  Output bytes: 15888605
  Input packets: 30896
  Output packets: 33607
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0

Logical interface fxp1.0 (Index 3) (SNMP ifIndex 14) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 7, Route table: 1
  Flags: Is-Primary
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 10/8, Local: 10.0.0.4, Broadcast: 10.255.255.255,
      Generation: 3
Protocol inet6, MTU: 1500, Generation: 8, Route table: 1
  Flags: Is-Primary
  Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::200:ff:fe00:4,
      Broadcast: Unspecified, Generation: 5
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: fec0::/64, Local: fec0::10:0:0:4, Broadcast: Unspecified,
      Generation: 7
Protocol tnp, MTU: 1500, Generation: 9, Route table: 1
  Flags: Primary, Is-Primary
  Addresses, Flags: None
    Destination: Unspecified, Local: 4, Broadcast: Unspecified,
      Generation: 8

show interfaces extensive (internal Ethernet [TX Matrix Plus Router])

user@host> show interfaces ixgbe0 extensive

Physical interface: ixgbe0, Enabled, Physical link is Up
  Interface index: 2, SNMP ifIndex: 116, Generation: 3
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags: Present Running
  Interface flags: SNMP-Traps
  Link type: Full-Duplex
  Physical info: Unspecified
  Hold-times: Up 0 ms, Down 0 ms
  Current address: 00:00:5E:00:53:04, Hardware address: 00:00:5E:00:53:04
  Alternate link address: Unspecified
  Last flapped: Never
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes: 242730780
Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes :  233127252
  Output bytes :  1269350897
  Input packets:  2398594
  Output packets:  4133510
IPv6 transit statistics:
  Input bytes :  0
  Output bytes :  0
  Input packets:  0
  Output packets:  0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

Logical interface ixgbe0.0 (Index 4) (SNMP ifIndex 117) (Generation 2)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes :  233127252
  Output bytes :  1269350897
  Input packets:  2398594
  Output packets:  4133510
IPv6 transit statistics:
  Input bytes :  0
  Output bytes :  0
  Input packets:  0
  Output packets:  0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

Interfaces Fundamentals for Routing Devices
show interfaces (PPPoE)

**Syntax**

```
show interfaces pp0.logical
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

(M120 routers, M320 routers, and MX Series routers only). Display status information about the PPPoE interface.

**Options**

- `pp0.logical`—Display standard status information about the PPPoE interface.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about PPPoE interfaces.
- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.
- `statistics`—(Optional) Display PPPoE interface statistics.

**Required Privilege**

`view`

**List of Sample Output**

- `show interfaces (PPPoE)` on page 1499
- `show interfaces (PPPoE over Aggregated Ethernet)` on page 1499
- `show interfaces brief (PPPoE)` on page 1500
- `show interfaces detail (PPPoE)` on page 1500
- `show interfaces extensive (PPPoE on M120 and M320 Routers)` on page 1501

**Output Fields**

Table 45 on page 1493 lists the output fields for the `show interfaces (PPPoE)` command. Output fields are listed in the approximate order in which they appear.

**Table 45: show interfaces (PPPoE) Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 45: show interfaces (PPPoE) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Physical interface type (PPPoE).</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation on the physical interface (PPPoE).</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link type</td>
<td>Physical interface link type: full duplex or half duplex.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the interface. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Input rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td>Output rate</td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td>Physical Info</td>
<td>Physical interface information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address of the hardware.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup address of the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 45: show interfaces (PPPoE) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> These fields include dropped traffic and exception traffic, as those fields are not separately defined.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Errors</strong>—Sum of incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Resource errors</strong>—Sum of B chip Tx drops and IXP Tx net transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), then the cable, the far-end system, or the PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Resource errors</strong>—Sum of B chip Tx drops and IXP Tx net transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**
### Table 45: show interfaces (PPPoE) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number (which reflects its initialization sequence).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Type of encapsulation configured on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>PPP parameters</td>
<td>PPP status:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• LCP restart timer—Length of time (in milliseconds) between successive Link Control Protocol (LCP) configuration requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NCP restart timer—Length of time (in milliseconds) between successive Network Control Protocol (NCP) configuration requests.</td>
<td></td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• State—State of the logical interface (up or down).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Session ID—PPPoE session ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Service name—Type of service required. Can be used to indicate an Internet service provider (ISP) name or a class or quality of service.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured AC name—Configured access concentrator name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Auto-reconnect timeout—Time after which to try to reconnect after a PPPoE session is terminated, in seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Idle Timeout—Length of time (in seconds) that a connection can be idle before disconnecting.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Underlying interface—Interface on which PPPoE is running.</td>
<td></td>
</tr>
<tr>
<td>Link</td>
<td>Name of the physical interfaces for member links in an aggregated Ethernet bundle for a PPPoE over aggregated Ethernet configuration. PPPoE traffic goes out on these interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 45: show interfaces (PPPoE) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</td>
<td></td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• interval seconds—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• down-count number—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• up-count number—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.</td>
<td></td>
</tr>
<tr>
<td>Keepalive statistics</td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input—Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (last seen 00:00:00 ago)—Time the last keepalive packet was received, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (last seen 00:00:00 ago)—Time the last keepalive packet was sent, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(MX Series routers with MPCs/MICs) When an MX Series router with MPCs/MICs is using PPP fast keepalive for a PPP link, the display does not include the number of keepalive packets received or sent, or the amount of time since the router received or sent the last keepalive packet.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
</tbody>
</table>
### Table 45: show interfaces (PPPoE) 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>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>none, detail, extensive</td>
</tr>
<tr>
<td>• Conf-ack-received—Acknowledgement was received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Conf-ack-sent—Acknowledgement was sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Conf-req-sent—Request was sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Down—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Not-configured—LCP is not configured on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Opened—LCP negotiation is successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail, extensive, none</td>
</tr>
<tr>
<td>• Conf-ack-received—Acknowledgement was received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Conf-ack-sent—Acknowledgement was sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Conf-req-sent—Request was sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Down—NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Not-configured—NCP is not configured on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Opened—NCP negotiation is successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>none, detail, extensive</td>
</tr>
<tr>
<td>• Chap-Chal-received—Challenge was received but response not yet sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chap-Chal-sent—Challenge was sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chap-Resp-received—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Chap-Resp-sent—Response was sent for the challenge received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Closed—CHAP authentication is incomplete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Failure—CHAP authentication failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Not-configured—CHAP is not configured on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Success—CHAP authentication was successful.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol family configured on the logical interface.</td>
<td>detail, extensive, none</td>
</tr>
<tr>
<td><strong>protocol-family</strong></td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>MTU size on the logical interface.</td>
<td>detail, extensive, none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Route table</strong></td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail, extensive, none</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail, extensive, none</td>
</tr>
</tbody>
</table>
Table 45: show interfaces (PPPoE) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses, Flags</td>
<td>Information about the addresses configured for the protocol family. Possible values are described in the &quot;Addresses Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces (PPPoE)

user@host> show interfaces pp0

Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type : Full-Duplex
  Link flags : None
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)

Logical interface pp0.0 (Index 72) (SNMP ifIndex 72)
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionDown, Session ID: None,
    Service name: None, Configured AC name: sapphire,
    Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
    Underlying interface: at-5/0/0.0 (Index 70)
  Input packets : 0
  Output packets: 0
  LCP state: Not-configured
  NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Closed
  Protocol inet, MTU: 100
  Flags: User-MTU, Negotiate-Address

show interfaces (PPPoE over Aggregated Ethernet)

user@host> show interfaces pp0.1073773821

Logical interface pp0.1073773821 (Index 80) (SNMP ifIndex 32584)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 1,
    Service name: None, Configured AC name: alcor, Remote MAC address: 00:00:5e:00:53:01,
    Underlying interface: demux0.100 (Index 88)
  Link:
show interfaces brief (PPPoE)

user@host> show interfaces pp0 brief

Physical interface: pp0, Enabled, Physical link is Up
Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps

Logical interface pp0.0
Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
PPPoE:
State: SessionDown, Session ID: None,
Service name: None, Configured AC name: sapphire,
Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
Underlying interface: at-5/0/0.0 (Index 70)
inet

show interfaces detail (PPPoE)

user@host> show interfaces pp0 detail

Physical interface: pp0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 24, Generation: 9
Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link type : Full-Duplex
Link flags : None
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Statistics last cleared: Never
Traffic statistics:
Input  bytes :                    0                    0 bps
Output bytes :                    0                    0 bps
Input  packets:                    0                    0 pps
Output packets:                    0                    0 pps

Logical interface pp0.0 (Index 72) (SNMP ifIndex 72) (Generation 14)
Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
PPPoE:
State: SessionDown, Session ID: None,
Service name: None, Configured AC name: sapphire,
Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
show interfaces extensive (PPPoE on M120 and M320 Routers)

user@host> show interfaces pp0 extensive

Physical interface: pp0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 93, Generation: 129
Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link type : Full-Duplex
Link flags : None
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Statistics last cleared: Never
Traffic statistics:
  Input bytes :  972192  0 bps
  Output bytes :  975010  0 bps
  Input packets:  1338  0 bps
  Output packets:  1473  0 bps
IPv6 transit statistics:
  Input bytes :  0
  Output bytes :  0
  Input packets:  0
  Output packets:  0

Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
  Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

Logical interface pp0.0 (Index 69) (SNMP ifIndex 96) (Generation 194)
  Flags: Point-To-Point SNMP-Traps Ox4000 Encapsulation: PPPoE
  PPPoE:
State: SessionUp, Session ID: 26,
Session AC name: None, AC MAC address: 00:00:5e:00:53:12,
Service name: None, Configured AC name: None,
Auto-reconnect timeout: Never, Idle timeout: Never,
Underlying interface: ge-3/0/1.0 (Index 67)

Traffic statistics:
Input bytes : 252
Output bytes : 296
Input packets: 7
Output packets: 8

IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes : 252
Output bytes : 296
Input packets: 7
Output packets: 8

Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
Input: 1 (last seen 00:00:00 ago)
Output: 1 (last sent 00:00:03 ago)
LCP state: Opened
CHAP state: Closed
PAP state: Closed
Protocol inet, MTU: 1492, Generation: 171, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
   Destination: 203.0.113.2, Local: 203.0.113.1, Broadcast: Unspecified, Generation: 206
show interfaces (PTX Series Packet Transport Routers)

Syntax

show interfaces et-fpc/pic/port
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>

Release Information

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 12.1 for PTX Series Packet Transport Routers.

Description

(PTX Series Packet Transport Routers only) Display status information about the specified Ethernet interface.

Options

et-fpc/pic/port—Display standard information about the specified Ethernet interface.
brief | detail | extensive | terse—(Optional) Display the specified level of output.
descriptions—(Optional) Display interface description strings.
media—(Optional) Display media-specific information about network interfaces.
snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.
statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces brief (PTX5000 Packet Transport Router) on page 1513
show interfaces extensive (PTX5000 Packet Transport Router) on page 1513
show interfaces terse (PTX5000 Packet Transport Router) on page 1514
show interfaces extensive (Junos OS Evolved) on page 1517

Output Fields

See Table 46 on page 1504 for the output fields for the show interfaces (PTX Series Packet Transport Routers) command.
### Table 46: show interfaces PTX Series Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>BPDU Error</td>
<td>Bridge protocol data unit (BPDU) errors (if any).</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC-Rewrite</td>
<td>MAC Rewrite errors (if any).</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of loopback: Local or Remote.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 46: show interfaces PTX Series Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>NOTE:</td>
<td>Input bytes and output bytes are counted as Layer 3 packet length.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td>Errors</td>
<td>Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td>Drops</td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Framing errors</td>
<td>Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td>Runt</td>
<td>Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td>Policed discards</td>
<td>Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td>L3 incompletes</td>
<td>Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the ignore-l3-incompletes statement.</td>
<td></td>
</tr>
<tr>
<td>NOTE:</td>
<td>The L3 incompletes field is not supported on PTX Series Packet Transport Routers.</td>
<td></td>
</tr>
<tr>
<td>L2 channel errors</td>
<td>Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td>L2 mismatch timeouts</td>
<td>Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td>FIFO errors</td>
<td>Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>Resource errors</td>
<td>Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 46: show interfaces PTX Series Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Carrier transitions—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Collisions—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aged packets—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FIFO errors—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HS link CRC errors—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MTU errors—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Egress queues</td>
<td>Total number of egress queues supported on the specified interface.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>(Egress)</td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Ingress queues</td>
<td>Total number of ingress queues supported on the specified interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Queue counters</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>(Ingress)</td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
</tbody>
</table>
Table 46: show interfaces PTX Series Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active alarms and</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Active defects</td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>• None—There are no active defects or alarms.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LOCAL-FAULT—Link fault signaling operates between the remote PHY RS (Reconciliation sub-layer) and the local RS. A Local Fault is used to signal a detected fault between the remote RS and the local RS to the local Ethernet interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• REMOTE-FAULT—When the Local Fault status reaches an RS, the RS stops sending MAC data and continuously generates the Remote Fault status on the transmit data path.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC statistics</td>
<td>Receive and Transmit statistics reported by the PIC’s MAC subsystem, including the following:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Total octets and</td>
<td>Total number of octets and packets.</td>
<td></td>
</tr>
<tr>
<td>total packets—Total number of octets and packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unicast packets,</td>
<td>Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td>Broadcast packets,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Multicast packets—Number of unicast, broadcast, and multicast packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• CRC/Align errors—</td>
<td>Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td>• FIFO error—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MAC control frames—Number of MAC control frames.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• MAC pause frames—Number of MAC control frames with pause operational code.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Oversized frames—Number of frames that exceed 1518 octets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Jabber frames—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Fragment frames—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• VLAN tagged frames—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Code violations—Number of times an event caused the PHY to indicate “Data reception error” or “Invalid data symbol error.”</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table 46: show interfaces PTX Series Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter statistics</td>
<td><strong>Receive</strong> and <strong>Transmit</strong> statistics reported by the PIC’s MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet’s source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet count</strong>—Number of packets received from the MAC hardware that the filter processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packet rejects</strong>—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input DA rejects</strong>—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the router from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local router (which the router is rejecting).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input SA rejects</strong>—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet count</strong>—Number of packets that the filter has given to the MAC hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet pad count</strong>—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packet error count</strong>—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CAM destination filters, CAM source filters</strong>—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 46: show interfaces PTX Series Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation information</td>
<td>Information about link autonegotiation.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Negotiation status:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Incomplete</strong>—Ethernet interface has the speed or link mode configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>No autonegotiation</strong>—Remote Ethernet interface has the speed or link mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configured, or does not perform autonegotiation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong>—Ethernet interface is connected to a device that performs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner status</strong>—<strong>OK</strong> when Ethernet interface is connected to a device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that performs autonegotiation and the autonegotiation process is successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link mode</strong>—Depending on the capability of the attached Ethernet device,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>either Full-duplex or Half-duplex.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Types of flow control supported by the remote Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device. For Fast Ethernet interfaces, the type is <strong>None</strong>. For Gigabit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethernet interfaces, types are <strong>Symmetric</strong> (link partner supports PAUSE on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receive and transmit), <strong>Asymmetric</strong> (link partner supports PAUSE on transmit),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and <strong>Symmetric/Asymmetric</strong> (link partner supports both PAUSE on receive and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmit or only PAUSE receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information from the link partner—<strong>Failure</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates a receive link error. <strong>OK</strong> indicates that the link partner is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receiving. <strong>Negotiation error</strong> indicates a negotiation error. <strong>Offline</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicates that the link partner is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local resolution</strong>—Information from the link partner:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Types of flow control supported by the remote Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device. For Gigabit Ethernet interfaces, types are <strong>Symmetric</strong> (link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>partner supports PAUSE on receive and transmit), <strong>Asymmetric</strong> (link partner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supports PAUSE on transmit), and <strong>Symmetric/Asymmetric</strong> (link partner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supports both PAUSE on receive and transmit or only PAUSE receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information. <strong>Link OK</strong> (no error detected on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receive), <strong>Offline</strong> (local interface is offline), and <strong>Link Failure</strong> (link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>error detected on receive).</td>
<td></td>
</tr>
</tbody>
</table>

| Packet Forwarding Engine        | Information about the configuration of the Packet Forwarding Engine:              | extensive       |
| configuration                   | • **Destination slot**—FPC slot number.                                           |                 |
Table 46: show interfaces PTX Series 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>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>• <strong>CoS transmit queue</strong></td>
<td>Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Bandwidth %</strong></td>
<td>Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Bandwidth bps</strong></td>
<td>Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Buffer %</strong></td>
<td>Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Buffer usec</strong></td>
<td>Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Priority</strong></td>
<td>Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Limit</strong></td>
<td>Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Index</strong></td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 46: show interfaces PTX Series 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-Tag</td>
<td>Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop—The outer VLAN tag of the incoming frame is removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap—The outer VLAN tag of the incoming frame is overwritten with the user-specified VLAN tag information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• push—An outer VLAN tag is pushed in front of the existing VLAN tag.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• push-push—Two VLAN tags are pushed in from the incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap-push—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• swap-swap—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user-specified VLAN tag value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop-swap—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pop-pop—Both the outer and inner VLAN tags of the incoming frame are removed.</td>
<td></td>
</tr>
<tr>
<td>Demux</td>
<td>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Source Family Inet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Destination Family Inet</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family. Possible values are described in the “Protocol Field” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Maximum labels</td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the specified interface set.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• input bytes, Output bytes—Number of bytes received and transmitted on the interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• input packets, Output packets—Number of packets received and transmitted on the interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: input bytes and output bytes are counted as Layer 3 packet length.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</td>
<td>extensive</td>
</tr>
<tr>
<td>Local statistics</td>
<td>Number and rate of bytes and packets destined to the router.</td>
<td>extensive</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>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Donor interface</td>
<td>(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Preferred source address</td>
<td>(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mac-Validate Failures</td>
<td>Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about flags (possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Sample Output

show interfaces brief (PTX5000 Packet Transport Router)

```
user@host> show interfaces brief et-7/0/0

Physical interface: et-7/0/0, Enabled, Physical link is Up
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
```

show interfaces extensive (PTX5000 Packet Transport Router)

```
user@host> show interfaces et-7/0/0 extensive

Physical interface: et-7/0/0, Enabled, Physical link is Up
Interface index: 168, SNMP ifIndex: 501, Generation: 171
Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 88:e0:f3:3b:de:43, Hardware address: 88:e0:f3:3b:de:43
Last flapped : 2012-01-18 11:48:24 PST (01:51:00 ago)
Statistics last cleared: 2012-01-18 13:38:54 PST (00:00:30 ago)
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 0 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
```
show interfaces terse (PTX5000 Packet Transport Router)

user@host> show interfaces terse

+------------+------------+------------+------------+------------+------------+------------+------------+
| Interface  | Admin Link | Proto      | Local      | Remote     |
|------------|------------|------------|------------|------------|------------|------------|------------|
| et-2/0/0   | up         | up         |            |            |            |            |            |
| et-2/0/1   | up         | up         |            |            |            |            |            |
| et-2/0/2   | up         | up         |            |            |            |            |            |
| et-2/0/3   | up         | up         |            |            |            |            |            |
| et-2/0/4   | up         | up         |            |            |            |            |            |
| et-2/0/5   | up         | down       |            |            |            |            |            |
| et-2/0/6   | up         | up         |            |            |            |            |            |
| et-2/0/7   | up         | up         |            |            |            |            |            |
| et-2/0/8   | up         | up         |            |            |            |            |            |
| et-2/0/9   | up         | down       |            |            |            |            |            |
| et-2/0/10  | up         | up         |            |            |            |            |            |
+------------+------------+------------+------------+------------+------------+------------+------------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status 1</th>
<th>Status 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>et-2/0/11</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/13</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-2/0/14</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/15</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/16</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/17</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-2/0/18</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-2/0/19</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/20</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-2/0/21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/0/22</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-2/0/23</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/2</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/4</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/5</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/8</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/9</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/10</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/11</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/13</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/14</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/15</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/16</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/17</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/18</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/19</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/20</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/21</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/22</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-2/1/23</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/0.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/0.32767</td>
<td>up</td>
<td>multiservice</td>
</tr>
<tr>
<td>et-5/0/1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/2</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/3</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/4</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/5</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/5.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/5.32767</td>
<td>up</td>
<td>multiservice</td>
</tr>
<tr>
<td>et-5/0/6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/8</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/9</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/10</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/11</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/12</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/13</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/14</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/15</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/16</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/17</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/18</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Interface</td>
<td>Status1</td>
<td>Status2</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>et-5/0/19</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/20</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/21</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-5/0/22</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/0/23</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-5/1/1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/2</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/3</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/4</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/5</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/6</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/7</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/8</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/9</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>et-7/0/10</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/11</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/12</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/13</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/14</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/15</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/16</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/17</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/18</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/19</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/20</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/21</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/22</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>et-7/0/23</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>dsc</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>em0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>em0.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>gre</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ipip</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ixgbe0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ixgbe0.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ixgbe1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>ixgbe1.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>lo0.0</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0.16384</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>lo0.16385</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>lsi</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
show interfaces extensive (Junos OS Evolved)

user@host> show interfaces et-0/0/0 extensive

Physical interface: et-0/0/0, Enabled, Physical link is Up
Interface index: 1002, SNMP ifIndex: 505, Generation: 113
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 100Gbps, BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Enabled
Device flags : Present Running
Interface flags: SNMP-Traps
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Damping : half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsuppressed
Current address: 88:e0:f3:3b:de:43, Hardware address: 88:e0:f3:3b:de:43
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 16045690984503098046 0 0
  1 16045690984503098046 0 0
  2 16045690984503098046 0 0
  3 16045690984503098046 0 0
Queue number: Mapped forwarding classes
  0 best-effort
  1 expedited-forwarding
  2 assured-forwarding
  3 network-control
Active alarms : None
Active defects : None
PCS statistics Seconds
Bit errors 0
<table>
<thead>
<tr>
<th>Error Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errored blocks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC statistics:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Filter statistics:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input packet count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Input SA rejects</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Output packet count</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Output packet pad count</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Output packet error count</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>CAM destination filters:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAM source filters:</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show interfaces (SONET/SDH)

Syntax

show interfaces so-fpc/pic/port
<br/>&lt;brief | detail | extensive | terse&gt;
<br/>&lt;descriptions&gt;
<br/>&lt;media&gt;
<br/>&lt;snmp-index snmp-index&gt;
<br/>&lt;statistics&gt;

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified SONET/SDH interface.

Options

so-fpc/pic/port—Display standard information about the specified SONET/SDH interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege

view

Related Documentation

• SONET/SDH Interfaces Overview

List of Sample Output

show interfaces (SDH Mode, PPP) on page 1532
show interfaces brief (SDH Mode, PPP) on page 1533
show interfaces detail (SDH Mode, PPP) on page 1533
show interfaces extensive (SDH Mode, PPP) on page 1534
show interfaces brief (SONET Mode, Frame Relay) on page 1536
show interfaces (SONET Mode, Frame Relay) on page 1537
show interfaces detail (SONET Mode, Frame Relay) on page 1537
show interfaces extensive (SONET Mode, Frame Relay) on page 1539
show interfaces extensive (OC768-over-4xOC192 Mode) on page 1539
show interfaces detail (IPv6 Tracking) on page 1545
show interfaces (Shared Interface) on page 1546

Output Fields

Table 47 on page 1520 lists the output fields for the show interfaces (SONET/SDH) command. Output fields are listed in the approximate order in which they appear.
Table 47: SONET/SDH show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface’s index number, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>SONET/SDH reference clock source: Internal or External. Clocking is configured and displayed only for channel 0.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Framing mode</strong></td>
<td>Framing mode: SONET or SDH.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Payload scrambler</td>
<td>Whether payload scrambling is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Device flags</strong></td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface flags</strong></td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Shared-interface</strong></td>
<td>Indicates whether the routing domain is the owner or non-owner of the shared interface. If the routing domain is the Root System Domain (RSD), the value is Owner. If the routing domain is a Protected System Domain (PSD) under the RSD, the value is Non-owner.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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>ANSI or ITU LMI</td>
<td>(Frame Relay) Settings for Local Management Interface (LMI). The format is (ANSI or ITU) LMI settings: value, value... xx seconds, where value can be:</td>
<td>All levels</td>
</tr>
<tr>
<td>settings</td>
<td>• n391dte—DTE full status polling interval (1-255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dce—DCE error threshold (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dte—DTE error threshold (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dce—DCE monitored event count (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dte—DTE monitored event count (1-10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t391dte—DTE polling timer (5-30 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t392dce—DCE polling verification timer (5-30 seconds)</td>
<td></td>
</tr>
<tr>
<td>LMI</td>
<td>Input: value (hh:mm:ss ago), Output: value (hh:mm:ss ago)</td>
<td>brief none</td>
</tr>
<tr>
<td>LMI statistics</td>
<td>(Frame Relay) LMI packet statistics:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input—Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input: nn (last seen hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output: nn (last sent hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td>DTE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE):</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Enquiries sent—Number of link status enquiries sent from the DTE to the DCE.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Full enquiries sent—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses received—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses received—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>DCE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Enquiries received—Number of enquiries received by the DCE from the DTE.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Full enquiries received—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses sent—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses sent—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 47: SONET/SDH show 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><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown messages received</strong>—Number of received packets that do not fall into any category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Asynchronous updates received</strong>—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Out-of-sequence packets received</strong>—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Keepalive responses timed out</strong>—Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay. Displayed only from the DTE) Number of DLCIs configured from the DCE.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Hold-times</strong></td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Keepalive settings</strong></td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- <strong>interval seconds</strong>—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>down-count number</strong>—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>up-count number</strong>—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.</td>
<td></td>
</tr>
<tr>
<td><strong>Keepalive or Keepalive statistics</strong></td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- <strong>Input</strong>—Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was received, in the format <em>hh:mm:ss</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Output</strong>—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was sent, in the format <em>hh:mm:ss</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-received</strong>—Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-sent</strong>—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong>—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not-configured</strong>—LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong>—LCP negotiation is successful.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 47: SONET/SDH show 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><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• Conf-ack-received</td>
<td>Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td>• Conf-ack-sent</td>
<td>Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td>• Conf-req-sent</td>
<td>Request was sent.</td>
<td></td>
</tr>
<tr>
<td>• Down</td>
<td>NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td>• Not-configured</td>
<td>NCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Opened</td>
<td>NCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• Chap-Chal-received</td>
<td>Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td>• Chap-Chal-sent</td>
<td>Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td>• Chap-Resp-received</td>
<td>Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td>• Chap-Resp-sent</td>
<td>Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td>• Closed</td>
<td>CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td>• Failure</td>
<td>CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td>• Not-configured</td>
<td>CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Success</td>
<td>CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Input rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Output rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number of bytes and packets received and transmitted on the physical interface, and the traffic rate in bits per seconds (bps).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>• Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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>Label-switched interface (LSI)</td>
<td>(Frame Relay) LSI traffic statistics:</td>
<td>extensive</td>
</tr>
<tr>
<td>traffic statistics</td>
<td>• Input bytes—Number of bytes and speed, in bits per second (bps), received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets and speed, in bps, transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

Input errors

Input errors on the interface whose definitions are as follows:

- **Errors**—Sum of the incoming frame aborts and FCS errors.
- **Drops**—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.
- **Framing errors**—Number of packets received with an invalid frame checksum (FCS).
- **Runts**—Number of frames received that are smaller than the runt threshold.
- **Giants**—Number of frames received that are larger than the giant threshold.
- **Bucket Drops**—Drops resulting from the traffic load exceeding the interface transmit/receive leaky bucket configuration. The default is **off**.
- **Policed discards**—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.
- **L3 incompletes**—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded.
- **L2 channel errors**—Number of times the software did not find a valid logical interface for an incoming frame.
- **L2 mismatch timeouts**—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.
- **H5 link CRC errors**—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.
- **H5 link FIFO overflows**—Number of FIFO overflows on the high-speed links between the ASICs responsible for handling the router interfaces.
Table 47: SONET/SDH show 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><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>H5 link FIFO underflows</strong>—Number of FIFO underflows on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeds the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>IPv6 transit statistics</strong></td>
<td>Number of transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Egress queues</strong></td>
<td>Total number of egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued packets</strong>—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dropped packets</strong>—Number of packets dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>SONET alarms</strong></td>
<td>(SONET) SONET media-specific alarms and defects that prevents the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SONET PHY, SONET section, SONET line, and SONET path.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>SONET defects</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Link</strong></td>
<td>(For 4-port OC192c PIC operating in OC768-over-4xOC192 mode) The link number. Errors and alarms are displayed for each link.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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><strong>SONET PHY</strong></td>
<td>Counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>PLL Lock</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>PHY Light</strong>—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td><strong>SONET section</strong></td>
<td>Counts of specific SONET errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BIP-B1</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>LOL</strong>—Loss of light</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ES-S</strong>—Errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SES-S</strong>—Severely errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SEFS-S</strong>—Severely errored framing seconds (section)</td>
<td></td>
</tr>
<tr>
<td><strong>SONET line</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BIP-B2</strong>—Bit interleaved parity for SONET line overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>REI-L</strong>—Remote error indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RDI-L</strong>—Remote defect indication (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AIS-L</strong>—Alarm indication signal (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ES-L</strong>—Errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SES-L</strong>—Severely errored seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UAS-L</strong>—Unavailable seconds (near-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>ES-LFE</strong>—Errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SES-LFE</strong>—Severely errored seconds (far-end line)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UAS-LFE</strong>—Unavailable seconds (far-end line)</td>
<td></td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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><strong>SONET path</strong></td>
<td>Active alarms and defects, plus counts of specific SONET errors with detailed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BIP-B3</strong>—Bit interleaved parity for SONET section overhead</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>REI-P</strong>—Remote error indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOP-P</strong>—Loss of pointer (path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS-P</strong>—Path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RDI-P</strong>—Path remote defect indication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UNEQ-P</strong>—Path unequipped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLM-P</strong>—Path payload (signal) label mismatch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-P</strong>—Errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-P</strong>—Severely errored seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-P</strong>—Unavailable seconds (near-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES-PFE</strong>—Errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES-PFE</strong>—Severely errored seconds (far-end STS path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS-PFE</strong>—Unavailable seconds (far-end STS path)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Received SONET overhead</strong></th>
<th>Values of the received and transmitted SONET overhead:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmitted SONET overhead</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>C2</strong>—Signal label. Allocated to identify the construction and content of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-level SPE and for PDI-P.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>F1</strong>—Section user channel byte. This byte is set aside for the purposes of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>K1</strong> and <strong>K2</strong>—These bytes are allocated for APS signaling for the protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the multiplex section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>J0</strong>—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used to transmit a 1-byte fixed-length string or a 16-byte message so that a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receiving terminal in a section can verify its continued connection to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>intended transmitter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>S1</strong>—Synchronization status. The S1 byte is located in the first STS-1 of an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-N.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Z3</strong> and <strong>Z4</strong>—Allocated for future use.</td>
<td></td>
</tr>
</tbody>
</table>

**SDH alarms**

**SDH defects**

SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: **SDH PHY**, **SDH regenerator section**, **SDH multiplex section**, and **SDH path**.

All levels
### Table 47: SONET/SDH show 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><strong>SDH PHY</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>PLL Lock</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>PHY Light</strong>—Loss of optical signal</td>
<td></td>
</tr>
<tr>
<td><strong>SDH regenerator section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RS-BIP8</strong>—24-bit BIP for multiplex section overhead (B2 bytes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>OOF</strong>—Out of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RS-ES</strong>—Errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RS-SES</strong>—Severely errored seconds (near-end regenerator section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RS-SEFS</strong>—Severely errored framing seconds (regenerator section)</td>
<td></td>
</tr>
<tr>
<td><strong>SDH multiplex section</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed information.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-BIP24</strong>—8-bit BIP for high-order path overhead (B3 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-FE-BE</strong>—Far-end block error (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-FERF</strong>—Far-end remote fail (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-AIS</strong>—Alarm indication signal (multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>BERR-SF</strong>—Bit error rate fault (signal failure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>BERR-SD</strong>—Bit error rate defect (signal degradation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-ES</strong>—Errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-SES</strong>—Severely errored seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-UAS</strong>—Unavailable seconds (near-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-ES-FE</strong>—Errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-SES-FE</strong>—Severely errored seconds (far-end multiplex section)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MS-UAS-FE</strong>—Unavailable seconds (far-end multiplex section)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 47: SONET/SDH show 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><strong>SDH path</strong></td>
<td>Active alarms and defects, plus counts of specific SDH errors with detailed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-BIP8</strong>—8-bit BIP for regenerator section overhead (B1 byte)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FEBE</strong>—Far-end block error (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-LOP</strong>—Loss of pointer (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-AIS</strong>—High-order-path alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-FERF</strong>—Far-end remote fail (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UNEQ</strong>—Unequipped (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-PLM</strong>—Payload label mismatch (high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES</strong>—Errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES</strong>—Severely errored seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS</strong>—Unavailable seconds (near-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-ES-FE</strong>—Errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-SES-FE</strong>—Severely errored seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HP-UAS-FE</strong>—Unavailable seconds (far-end high-order path)</td>
<td></td>
</tr>
<tr>
<td>**Received SDH</td>
<td>Values of the received and transmitted SONET overhead:</td>
<td>extensive</td>
</tr>
<tr>
<td>overhead** Transmitted SDH</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>overhead</strong></td>
<td>• <strong>C2</strong>—Signal label. Allocated to identify the construction and content of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-level SPE and for PDI-P.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>F1</strong>—Section user channel byte. This byte is set aside for the purposes of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>K1</strong> and <strong>K2</strong>—These bytes are allocated for APS signaling for the protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the multiplex section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>J0</strong>—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used to transmit a 1-byte fixed-length string or a 16-byte message so that a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receiving terminal in a section can verify its continued connection to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>intended transmitter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>S1</strong>—Synchronization status. The S1 byte is located in the first STS-1 of an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STS-N.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Z3</strong> and <strong>Z4</strong>—Allocated for future use.</td>
<td></td>
</tr>
<tr>
<td><strong>Received path trace</strong></td>
<td>SONET/SDH interfaces allow path trace bytes to be sent inband across the</td>
<td>extensive</td>
</tr>
<tr>
<td>**Transmitted path</td>
<td>SONET/SDH link. Juniper Networks and other router manufacturers use these bytes</td>
<td></td>
</tr>
<tr>
<td><strong>trace</strong></td>
<td>to help diagnose misconfigurations and network errors by setting the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmitted path trace message so that it contains the system hostname and name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the physical interface. The received path trace value is the message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>received from the router at the other end of the fiber. The transmitted path trace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>value is the message that this router transmits.</td>
<td></td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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>HDLC configuration</td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Policing bucket—Configured state of the receiving policer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shaping bucket—Configured state of the transmitting shaper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Giant threshold—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runt threshold—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td>CoS information</td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding Engine configuration</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Destination slot—FPC slot number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PLP byte—Packet Level Protocol byte.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the &quot;Logical Interface Flags&quot; section under &quot;Common Output Fields Description&quot; on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>PPP parameters</td>
<td>The PPP loopback clear timer value.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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><strong>Shared interface</strong></td>
<td>Provides the following information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• shared with—(RSD only) Indicates which PSD owns the logical shared interface. For example, psd3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• peer interface—(PSD only) Lists the logical tunnel interface that peers with the logical shared interface. For example, ut-2/1/0.2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• tunnel token—Specifies the receive (RX) and transmit (TX) tunnel tokens. For example, Rx: 5.519, Tx: 13.514.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, or mpls.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Multilink bundle</td>
<td>(If the logical interface is configured as part of a multilink bundle.) Interface name for the multilink bundle.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>AS bundle</td>
<td>(If the logical interface is configured as part of an aggregated SONET bundle.) AS bundle number.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 47: SONET/SDH show 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>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Active—Set when the link is active and the DTE and DCE are exchanging information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Set when the link is active, but no information is received from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unconfigured—Set when the corresponding DLCI in the DCE is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured—Set when the corresponding DLCI in the DCE is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dce-configured—Displayed when the command is issued from the DTE.</td>
<td></td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active DLCI—Number of active DLCIs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inactive DLCI—Number of inactive DLCIs.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show interfaces (SDH Mode, PPP)

```
user@host> show interfaces so-0/0/0
Physical interface: so-0/0/0, Enabled, Physical link is Up
   Interface index: 149, SNMP ifIndex: 66
   Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
   Loopback: None, FCS: 16, Payload scrambler: Enabled
   Device flags  : Present Running
   Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
   Link flags     : Keepalives
   Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
   Keepalive: Input: 30 (00:00:07 ago), Output: 29 (00:00:05 ago)
   LCP state: Opened
   CHAP state: Closed
   CoS queues     : 4 supported, 4 maximum usable queues
   Last flapped   : 2006-03-24 13:20:56 PST (00:05:09 ago)
   Input rate     : 0 bps (0 pps)
   Output rate    : 0 bps (0 pps)
   SDH alarms     : None
   SDH defects     : None
```
show interfaces brief (SDH Mode, PPP)

```bash
user@host> show interfaces so-0/0/0 brief
Physical interface: so-0/0/0, Enabled, Physical link is Up
Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 25 (00:00:01 ago), Output: 24 (00:00:04 ago)
SDH alarms : None
SDH defects : None

Logical interface so-0/0/0.0
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
inet  10.0.12.1/30
iso
mpls
```

show interfaces detail (SDH Mode, PPP)

```bash
user@host> show interfaces so-0/0/0 detail
Physical interface: so-0/0/0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 66, Generation: 35
Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Hold-times : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 33 (last seen 00:00:05 ago)
  Output: 32 (last sent 00:00:06 ago)
LCP state: Opened
CHAP state: Closed
CoS queues : 4 supported, 4 maximum usable queues
Last flapped : 2006-03-24 13:20:56 PST (00:05:38 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 862  0 bps
  Output bytes : 3592  64 bps
```
show interfaces extensive (SDH Mode, PPP)

user@host> show interfaces so-0/0/0 extensive

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 149, SNMP ifIndex: 66, Generation: 35
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags    : Keepalives
  Hold-times    : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input: 36 (last seen 00:00:01 ago)
    Output: 35 (last sent 00:00:10 ago)
  LCP state: Opened
  CHAP state: Closed
  CoS queues    : 4 supported, 4 maximum usable queues
  Last flapped  : 2006-03-24 13:20:56 PST (00:06:08 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes  : 922                  0 bps
    Output bytes : 3850                 64 bps
    Input packets: 75                   0 bps
    Output packets: 356                  0 bps
  Label-switched interface (LSI) traffic statistics:
    Input bytes  : 0                    0 bps
    Input packets: 0                    0 bps
    Input errors:   

showinterfacesextensive(SDHMode,PPP)
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Bucket drops: 0, Policed discards: 218, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 2, HS link CRC errors: 0, HS link FIFO overflows: 0

Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO underflows: 0, MTU errors: 0

Egress queues: 4 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>354</td>
<td>354</td>
<td>0</td>
</tr>
</tbody>
</table>

SDH alarms: None
SDH defects: None

SDH PHY:

<table>
<thead>
<tr>
<th>SDH PHY:</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL Lock</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>PHY Lock</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>

SDH regenerator section:

<table>
<thead>
<tr>
<th>SDH regenerator</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS-BIP8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>OOF</td>
<td>3</td>
<td>8</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>3</td>
<td>2</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>3</td>
<td>2</td>
<td>OK</td>
</tr>
<tr>
<td>RS-ES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS-SES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SDH multiplex section:

<table>
<thead>
<tr>
<th>SDH multiplex</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-BIP24</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>MS-FEBE</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>MS-FERF</td>
<td>3</td>
<td>2</td>
<td>OK</td>
</tr>
<tr>
<td>MS-AIS</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>BERR-SF</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BERR-SD</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>MS-ES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-SES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-SES-FE</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-UAS-FE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SDH path:

<table>
<thead>
<tr>
<th>SDH path:</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-BIP8</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>HP-FEBE</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>HP-LOP</td>
<td>1</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>HP-AIS</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>HP-FERF</td>
<td>3</td>
<td>2</td>
<td>OK</td>
</tr>
<tr>
<td>HP-UNEQ</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>HP-PLM</td>
<td>1</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>HP-ES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-SES</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-ES-FE</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-SES-FE</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP-UAS-FE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Received SDH overhead:

<table>
<thead>
<tr>
<th>F1</th>
<th>S1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00, J0</td>
<td>0x00, 0x00, K1</td>
</tr>
<tr>
<td>0x00, C2</td>
<td>0xcf, C2(cmp)</td>
</tr>
</tbody>
</table>
show interfaces brief (SONET Mode, Frame Relay)

Physical interface: so-0/0/0, Enabled, Physical link is Up
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 29 (00:00:02 ago), Output: 28 (00:00:01 ago)
SONET alarms : None
SONET defects : None

Logical interface so-0/0/0.0 (Index 66) (SNMP ifIndex 43) (Generation 19)
Flags: Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
PPP parameters:
PPP loopback clear timer: 3 sec
Protocol inet, MTU: 4470, Generation: 48, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.0.12.0/30, Local: 10.0.12.1, Broadcast: 10.0.12.3, Generation: 48
Protocol iso, MTU: 4470, Generation: 49, Route table: 0
  Flags: Protocol-Down
Protocol mpls, MTU: 4458, Maximum labels: 3, Generation: 50, Route table: 0
  Flags: Protocol-Down, Is-Primary
MS-ES-FE                  3
show interfaces brief (SONET Mode, Frame Relay)

Interfaces Fundamentals for Routing Devices
show interfaces (SONET Mode, Frame Relay)

user@host> show interfaces so-0/0/0

Physical interface: so-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 66
Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, SONET mode,
Speed: OC3, Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 23 (00:00:05 ago), Output: 22 (00:00:03 ago)
DTE statistics:
  Enquiries sent : 19
  Full enquiries sent : 3
  Enquiry responses received : 20
  Full enquiry responses received : 3
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 1
CoS queues : 4 supported, 4 maximum usable queues
Last flapped : 2006-03-06 11:53:20 PST (3d 03:09 ago)
Input rate : 0 bps (0 pps)
Output rate : 56 bps (0 pps)
SONET alarms : None
SONET defects : None

Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Input packets : 0
Output packets: 0
Protocol inet, MTU: 4470
  Flags: None
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.0.12.2, Local: 10.0.12.1
Protocol iso, MTU: 4470
  Flags: None
Protocol mpls, MTU: 4450, Maximum labels: 3
DLCI 16
  Flags: Down, DCE-Unconfigured
  Total down time: 00:03:11 sec, Last down: 00:03:11 ago
    Input packets : 0
    Output packets: 0
DLCI statistics:
  Active DLCI :0 Inactive DLCI :1

show interfaces detail (SONET Mode, Frame Relay)

user@host> show interfaces so-0/0/0 detail

Physical interface: so-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 66, Generation: 11
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives DTE
Hold-times : Up 0 ms, Down 0 ms
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI statistics:
  Input : 33 (last seen 00:00:09 ago)
  Output: 32 (last sent 00:00:01 ago)
DTE statistics:
  Enquiries sent : 27
  Full enquiries sent : 5
  Enquiry responses received : 28
  Full enquiry responses received : 5
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 1
CoS queues : 4 supported, 4 maximum usable queues
Last flapped : 2006-03-06 11:53:20 PST (3d 03:10 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 495368 0 bps
  Output bytes : 2765014 56 bps
  Input packets: 41165 0 pps
  Output packets: 133530 0 pps
Egress queues: 4 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort  18          18          0
  1 expedited-fo 0            0          0
  2 assured-forw 0            0          0
  3 network-cont 133506      133506       0
SONET alarms : None
SONET defects : None
Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43) (Generation 28)
  Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
show interfaces extensive (SONET Mode, Frame Relay)

user@host> show interfaces so-0/0/0 extensive

Physical interface: so-0/0/0, Enabled, Physical link is Up
- Interface index: 128, SNMP ifIndex: 66, Generation: 11
- Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, SONET mode,
- Speed: OC3, Loopback: None, FCS: 16, Payload scrambler: Enabled
- Device flags : Present Running
- Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
- Link flags : Keepalives DTE
- Hold-times : Up 0 ms, Down 0 ms
- ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds

LMI statistics:
- Input : 39 (last seen 00:00:02 ago)
- Output: 36 (last sent 00:00:07 ago)

DTE statistics:
- Enquiries sent : 30
- Full enquiries sent : 6
- Enquiry responses received : 33
- Full enquiry responses received : 6

DCE statistics:
- Enquiries received : 0
- Full enquiries received : 0
- Enquiry responses sent : 0
- Full enquiry responses sent : 0

Common statistics:
- Unknown messages received : 0
- Asynchronous updates received : 0
- Out-of-sequence packets received : 0
- Keepalive responses timedout : 1

CoS queues : 4 supported, 4 maximum usable queues
Last flapped : 2006-03-06 11:53:20 PST (3d 03:11 ago)
Statistics last cleared: Never

Traffic statistics:
- Input bytes : 495452 56 bps
- Output bytes : 2765074 0 bps
- Input packets: 41171 0 pps
Output packets: 133534 0 pps
Label-switched interface (LSI) traffic statistics:
Input bytes : 0 0 bps
Input packets: 0 0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Bucket drops: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, HS link CRC errors: 0, HS link FIFO overflows: 0
Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO underflows: 0, MTU errors: 0
Egress queues: 4 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
<table>
<thead>
<tr>
<th></th>
<th>0 best-effort</th>
<th>1 expedited-fo</th>
<th>2 assured-forward</th>
<th>3 network-cont</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued packets</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>133510</td>
</tr>
<tr>
<td>Transmitted packets</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>133510</td>
</tr>
<tr>
<td>Dropped packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SONET alarms : None
SONET defects : None
SONET PHY:
<table>
<thead>
<tr>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL Lock</td>
<td>0</td>
<td>0 OK</td>
</tr>
<tr>
<td>PHY Light</td>
<td>60</td>
<td>1 OK</td>
</tr>
</tbody>
</table>
SONET section:
| BIP-B1 | 0 | 0 |
| SEF | 108 | 158 OK |
| LOS | 108 | 2 OK |
| LOF | 108 | 2 OK |
| ES-S | 108 |
| SES-S | 108 |
| SEFS-S | 108 |
SONET line:
| BIP-B2 | 0 | 0 |
| REI-L | 0 | 0 |
| RDI-L | 1 | 1 OK |
| AIS-L | 107 | 1 OK |
| BERR-SF | 0 | 0 OK |
| BERR-SD | 44 | 2 OK |
| ES-L | 108 |
| SES-L | 108 |
| UAS-L | 97 |
| ES-LFE | 1 |
| SES-LFE | 1 |
| UAS-LFE | 0 |
SONET path:
| BIP-B3 | 0 | 0 |
| REI-P | 0 | 0 |
| LOP-P | 1 | 1 OK |
| AIS-P | 107 | 1 OK |
| RDI-P | 1 | 1 OK |
| UNEQ-P | 0 | 0 OK |
| PLM-P | 1 | 1 OK |
| ES-P | 108 |
| SES-P | 108 |
| UAS-P | 97 |
ES-PFE                    1
SES-PFE                   1
UAS-PFE                   0

Received SONET overhead:
F1  : 0x00, J0  : 0x00, K1  : 0x00, K2  : 0x00
S1  : 0x00, C2  : 0xcf, C2(cmp) : 0xcf, F2  : 0x00
Z3  : 0x00, Z4  : 0x00, S1(cmp) : 0x00

Transmitted SONET overhead:
F1  : 0x00, J0  : 0x01, K1  : 0x00, K2  : 0x00
S1  : 0x00, C2  : 0xcf, F2  : 0x00, Z3  : 0x00
Z4  : 0x00

Received path trace: R2 so-0/0/0
S2 32 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00   R2 so-0/0/0....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............

Transmitted path trace: R1 so-0/0/0
S2 31 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00   R1 so-0/0/0....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..............

HDLC configuration:
Policing bucket: Disabled
Shaping bucket: Disabled
Giant threshold: 4484, Runt threshold: 3

Packet Forwarding Engine configuration:
Destination slot: 0, PLP byte: 1 (0x00)

CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>95 %</td>
<td>147744000</td>
<td>95 %</td>
<td>low</td>
</tr>
<tr>
<td>network-control</td>
<td>3</td>
<td>7776000</td>
<td>5</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43) (Generation 28)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID

Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Transit statistics:
Input bytes : 0 bps
Output bytes : 0 bps
Input packets: 0 pps
Output packets: 0 pps

Protocol inet, MTU: 4470, Generation: 49, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
   Destination: 10.0.12.2, Local: 10.0.12.1, Broadcast: Unspecified,
   Generation: 61
Protocol iso, MTU: 4470, Generation: 50, Route table: 0
Flags: None
Protocol mpls, MTU: 4450, Maximum labels: 3, Generation: 51, Route table: 0
DLCI 16
Flags: Down, DCE-Unconfigured
show interfaces extensive (OC768-over-4xOC192 Mode)

```
user@host> show interfaces so-7/0/0 extensive

Physical interface: so-7/0/0, Enabled, Physical link is Up
Interface index: 163, SNMP ifIndex: 23, Generation: 186
Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC768,
Loopback: Local, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : No-Keepalives
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2006-01-13 10:43:39 PST (01:05:33 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 76992                      200 bps
Output bytes : 83707                     216 bps
Input packets: 1343                      0 pps
Output packets: 1343                     0 pps
Input errors:
   Errors: 0, Drops: 3885, Framing errors: 68154624, Runts: 0, Giants: 0, Bucket drops: 0,
   Policed discards: 0, L3 incompletes: 95040248, L2 channel errors: 0, L2 mismatch timeouts: 0,
   HS link CRC errors: 0, HS link FIFO overflows: 30742070
Output errors:
   Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO underflows: 0,
   MTU errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort 2 2 0
  1 expedited-fo 0 0 0
  2 assured-forw 0 0 0
  3 network-cont 1341 1341 0

SONET alarms : None
SONET defects : None
Link : 0
SONET alarms : None
SONET defects : None
SONET PHY: Seconds Count State
  PLL Lock 0 0 OK
  PHY Light 0 0 OK
SONET section:
```

<table>
<thead>
<tr>
<th></th>
<th>Line</th>
<th>Path</th>
<th>Path Trace</th>
<th>Payload Pointer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BIP-B1</td>
<td>SEF</td>
<td>LOS</td>
<td>LOF</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1 OK</td>
<td>0</td>
<td>2 OK</td>
</tr>
<tr>
<td></td>
<td>ES-S</td>
<td>SES-S</td>
<td>SEFS-S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>BIP-B2</td>
<td>0</td>
<td>0</td>
<td>REI-L</td>
<td>RDI-L</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>AIS-L</td>
<td>BERR-SF</td>
<td>BERR-SD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1 OK</td>
</tr>
<tr>
<td></td>
<td>ES-L</td>
<td>SES-L</td>
<td>UAS-L</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SES-LFE</td>
<td>UAS-LFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>BIP-B3</td>
<td>0</td>
<td>0</td>
<td>REI-P</td>
<td>LOP-P</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>AIS-P</td>
<td>RDI-P</td>
<td>UNEQ-P</td>
<td>PLM-P</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ES-P</td>
<td>SES-P</td>
<td>UAS-P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SES-PFE</td>
<td>UAS-PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current pointer</td>
<td>522</td>
<td>Pointer increment count</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Pointer decrement count</td>
<td>0</td>
<td>New pointer NDF count</td>
<td>0</td>
</tr>
<tr>
<td>BIP-B2</td>
<td>BIP-B3</td>
<td>Payload pointer</td>
<td>522</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Pointer increment count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>New pointer NDF count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Link</td>
<td>1</td>
<td>SONET alarms  : None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>SONET defects : None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## SONET PHY:

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL Lock</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>PHY Light</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

## SONET section:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BIP-B1</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>SEF</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>3</td>
<td>2</td>
<td>OK</td>
</tr>
<tr>
<td>ES-S</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES-S</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEFS-S</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## SONET line:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BIP-B2</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>REI-L</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RDI-L</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>AIS-L</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>BERR-SF</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BERR-SD</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>ES-L</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES-L</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS-L</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES-LFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES-LFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS-LFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## SONET path:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BIP-B3</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>REI-P</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LOP-P</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>AIS-P</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>RDI-P</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>UNEQ-P</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>PLM-P</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>ES-P</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES-P</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS-P</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES-PFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES-PFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS-PFE</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Payload pointer:
- **Current pointer**: 522
- **Pointer increment count**: 0
- **Pointer decrement count**: 0
- **New pointer NDF count**: 0

### Received SONET overhead:

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Ox00, J1</td>
<td>Ox01, K1</td>
<td>Ox00, K2</td>
<td>Ox00</td>
</tr>
<tr>
<td>S1</td>
<td>Ox00, C2</td>
<td>Oxcf, C2(cmp)</td>
<td>Oxcf, F2</td>
<td>Ox00</td>
</tr>
<tr>
<td>Z3</td>
<td>Ox00, Z4</td>
<td>Ox00, S1(cmp)</td>
<td>Ox00</td>
<td></td>
</tr>
</tbody>
</table>

### Transmitted SONET overhead:

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>Ox00, J1</td>
<td>Ox01, K1</td>
<td>Ox00, K2</td>
<td>Ox00</td>
</tr>
<tr>
<td>S1</td>
<td>Ox00, C2</td>
<td>Oxcf, F2</td>
<td>Ox00, Z3</td>
<td>Ox00</td>
</tr>
<tr>
<td>Z4</td>
<td>Ox00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Received path trace:

```
66 6f 6c 64 20 73 6f 2d 37 2f 30 00 00 00 0d 0a
```

### Transmitted path trace:

```
66 6f 6c 64 20 73 6f 2d 37 2f 30 00 00 00 0d 0a
```
show interfaces detail (IPv6 Tracking)

```
user@host> show interfaces so-0/2/0 detail

Physical interface: so-0/2/0, Enabled, Physical link is Up
    Interface index: 130, SNMP ifIndex: 26, Generation: 131
    Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
    Loopback: None, FCS: 16, Payload scrambler: Enabled
    Device flags : Present Running
    Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
    Link flags : Keepalives
    Hold-times : Up 0 ms, Down 0 ms
    Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
    Keepalive statistics:
      Input : 7 (last seen 00:00:01 ago)
      Output: 6 (last sent 00:00:08 ago)
    LCP state: Opened
    CHAP state: Closed
    CoS queues : 4 supported, 4 maximum usable queues
    Last flapped : 2007-11-29 08:45:47 PST (1d 03:44 ago)
    Statistics last cleared: Never
    Traffic statistics:
      Input  bytes  :              7407782                   40 bps
      Output bytes  :              7307322                   48 bps
      Input  packets:               107570                    0 pps
      Output packets:               108893                    0 pps
    IPv6 transit statistics:
      Input  bytes  :               57328
      Output bytes  :               57400
      Input  packets:                1024
      Output packets:                1025
    Egress queues: 4 supported, 4 in use
    Queue counters:        Queued packets Transmitted packets Dropped packets
      0 best-effort        1191            1191              0
      1 expedited-fo       0              0                  0
      2 assured-forw       0              0                  0
      3 network-cont       107700          107700            0
    SONET alarms : None
    SONET defects : None

Logical interface so-0/2/0.0 (Index 70) (SNMP ifIndex 47) (Generation 231)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
    Protocol inet6, MTU: 4470, Generation: 433, Route table: 0
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 2001:db8::2:1/32, Local: 2001:db8::2:2,
      Broadcast: Unspecified, Generation: 683
    Addresses, Flags: Is-Preferred
      Destination: 2001:db8::1:2, Local: 2001:db8::1:3,
      Broadcast: Unspecified, Generation: 684
```
show interfaces (Shared Interface)

user@rsd1> show interfaces so-7/2/0

Physical interface: so-7/2/0, Enabled, Physical link is Down
Interface index: 128, SNMP ifIndex: 109
Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, SONET mode,
Speed: OC192, Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps Internal: 0x4000
Shared-interface : Owner
Link flags : No-Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 0 (never), Output: 0 (never)
DTE statistics:
  Enquiries sent : 0
  Full enquiries sent : 0
  Enquiry responses received : 0
  Full enquiry responses received : 0
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 0
  CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2008-08-11 10:51:51 PDT (1w1d 04:47 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
SONET alarms : LOL, PLL
SONET defects : LOL, PLL, LOF, SEF, AIS-L, AIS-P

Logical interface so-7/2/0.0 (Index 67) (SNMP ifIndex 117)
Flags: Device-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: FR-NLPII
Shared interface:
  Shared with: psd5
  Tunnel token: Rx: 2.517, Tx: 1.517
Input packets : 0
Output packets: 0
DLCI 700
Flags: Active
  Total down time: 00:01:09 sec, Last down: 284:58:21 ago
  Input packets : 0
  Output packets: 0
DLCI statistics:
  Active DLCI : 1 Inactive DLCI : 0
show interfaces (Serial)

**Syntax**

```show interfaces interface-type
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Display status information about serial interfaces, including RS-232, RS-422/449, EIA-530, X.21, and V.35.

**Options**

- `interface-type`—On M Series and T Series routers, the interface type is `se-fpc/pic/port`.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

**Required Privilege**

- view

**List of Sample Output**

- `show interfaces (Serial, EIA-530)` on page 1553
- `show interfaces brief (Serial, EIA-530)` on page 1553
- `show interfaces detail (Serial, EIA-530)` on page 1554
- `show interfaces extensive (Serial, EIA-530)` on page 1554
- `show interfaces (Serial, V.35)` on page 1556
- `show interfaces brief (Serial, V.35)` on page 1556
- `show interfaces detail (Serial, V.35)` on page 1556
- `show interfaces extensive (Serial, V.35)` on page 1557
- `show interfaces statistics detail (RS 449)` on page 1558

**Output Fields**

Table 48 on page 1547 lists the output fields for the `show interfaces` (Serial) 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>Physical Interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 48: show interfaces (Serial) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>Maximum speed. The nonconfigurable value is 16,384 kbps.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalive packets.</td>
<td>All levels</td>
</tr>
<tr>
<td>• Interval seconds</td>
<td>Time between successive keepalive requests. The range of values, in seconds, is 10 to 32,767. The default value is 10.</td>
<td></td>
</tr>
<tr>
<td>• Up-count number</td>
<td>Number of keepalive packets a destination must receive to change a link’s status from down to up. The range of values is 1 to 255. The default value is 1.</td>
<td></td>
</tr>
<tr>
<td>• Down-count number</td>
<td>Number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 to 255. The default value is 3.</td>
<td></td>
</tr>
<tr>
<td>Keepalive</td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>brief</td>
</tr>
<tr>
<td>• Input: number (hh:mm:ss ago)</td>
<td>Number of keepalive packets received by PPP and the time since the last keepalive packet was received.</td>
<td></td>
</tr>
<tr>
<td>• Output: number (hh:mm:ss ago)</td>
<td>Number of keepalive packets sent by PPP and the time since the last keepalive packet was sent.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 48: `show interfaces (Serial)` 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>Keepalive statistics</strong></td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input:</strong> <code>number (last seen hh:mm:ss ago)</code> — Number of keepalive packets received by PPP and the time since the last keepalive packet was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output:</strong> <code>number (last seen hh:mm:ss ago)</code> — Number of keepalive packets sent by PPP and the time since the last keepalive packet was sent.</td>
<td></td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-received</strong> — Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-sent</strong> — Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-req-sent</strong> — Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong> — LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong> — LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Opened</strong> — LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-received</strong> — Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-ack-sent</strong> — Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Conf-req-sent</strong> — Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong> — NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong> — NCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Opened</strong> — NCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-received</strong> — Challenge was received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Chal-sent</strong> — Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-received</strong> — Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chap-Resp-sent</strong> — Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong> — CHAP authentication is incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Failure</strong> — CHAP authentication failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Not-configured</strong> — CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong> — CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is <code>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</code>. For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Input Rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Output Rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>None specified</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><strong>Statistics last cleared</strong></td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Input errors</strong></td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>.</td>
<td>This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeds the MTU of the interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Egress queues supported</strong></td>
<td>Total number of egress queues supported on the specified interface. Displayed with the <strong>statistics</strong> option.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td><strong>Egress queues in use</strong></td>
<td>Total number of egress queues in use on the specified interface. Displayed with the <strong>statistics</strong> option.</td>
<td><strong>detail extensive</strong></td>
</tr>
</tbody>
</table>
### Table 48: show interfaces (Serial) 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>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Displayed with the <strong>statistics</strong> option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued packets</strong>—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dropped packets</strong>—Number of packets dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>Serial media information</strong></td>
<td>Information about the physical media:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Line protocol</strong>—eia530, eia530a, rs232, rs449, v.35, or x.21.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resync history</strong>—Information about resynchronization events:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Sync loss count</strong>—Number of times the synchronization was lost.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Data signal</strong>—(X.21 and V.35) Information about the data signal:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Rx Clock</strong>—Receive clock status: OK (DTE is receiving the receive clock signal) or Not detected (receive clock signal is not being received).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Control signals</strong>—Information about modem control signals:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local mode</strong>—DCE (data communication equipment) or DTE (data terminal equipment)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>To DCE</strong>—Control signals that the Serial PIC sent to the DCE: DTR (Data Terminal Ready: <strong>up</strong> or <strong>down</strong>) or RTS (Request To Send: <strong>up</strong> or <strong>down</strong>.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>From DCE</strong>—Control signals that the Serial PIC received from the DCE: CTS (Clear To Send: <strong>up</strong> or <strong>down</strong>), DCD (Data Carrier Detect: <strong>up</strong> or <strong>down</strong>), DSR (Data Set Ready: <strong>up</strong> or <strong>down</strong>), or TM (Test Mode: <strong>up</strong> or <strong>down</strong>).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Clocking mode</strong>—Clocking used for the transmit clock:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>dte</strong>—Transmit clock is generated by DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>dce</strong>—Transmit clock is generated by the DCE and is looped back as the transmit clock.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>loop-timed</strong>—Receive clock from the DCE is looped back as the transmit clock.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Clock rate</strong>—Rate, in megahertz (MHz), at which the clock is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Loopback</strong>—Configured loopback mode for the interface: <strong>dce-remote</strong>, <strong>dce-local</strong>, liu, local, or none.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Tx clock</strong>—Clocking phase of the transmit clock: <strong>invert</strong> (transmit clock polarity is inverted) or <strong>non-invert</strong> (transmit clock polarity is not inverted).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Line encoding</strong>—Type of line encoding used: <strong>nrz</strong> (nonreturn to zero) or <strong>nrzi</strong> (return to zero inverted).</td>
<td></td>
</tr>
<tr>
<td><strong>Packet Forwarding Engine</strong></td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td>configuration</td>
<td>• <strong>Destination slot</strong>—FPC slot number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLP byte</strong>—Packet Level Protocol byte.</td>
<td></td>
</tr>
</tbody>
</table>


Table 48: show interfaces (Serial) 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>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• CoS transmit queue—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth %—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bandwidth bps—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer %—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buffer usec—Amount of buffer space allocated to the queue, in microseconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Priority—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Name of the logical interface.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the source and destination address are also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, mpls.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 48: show interfaces (Serial) Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces (Serial, EIA-530)

```
user@host> show interfaces se-5/0/1
Physical interface: se-5/0/1, Enabled, Physical link is Up
Interface index: 144, SNMP ifIndex: 41
Type: Serial, Link-level type: PPP, MTU: 1504, Maximum speed: 16384kbps
Device flags : Present Running
Interface flags: Point-To-Point Internal: 0x4000
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 32 (00:00:10 ago), Output: 31 (00:00:07 ago)
LCP state: Opened
CHAP state: Closed
CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2006-04-26 15:10:18 PDT (00:00:22 ago)
Input rate : 0 bps (0pps)
Output rate : 0 bps (0pps)
Logical interface se-5/0/1.0 (Index 71) (SNMP ifIndex 45)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Protocol inet, MTU: 1500
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 12.0.0.0/30, Local: 12.0.0.1, Broadcast: 12.0.0.3
```

show interfaces brief (Serial, EIA-530)

```
user@host> show interfaces se-5/0/1 brief
Physical interface: se-5/0/1, Enabled, Physical link is Up
Type: Serial, Link-level type: PPP, MTU: 1504
Device flags : Present Running
Interface flags: Point-To-Point Internal: 0x4000
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 235 (00:00:10 ago), Output: 234 (00:00:00 ago)
```

Copyright © 2019, Juniper Networks, Inc.
Logical interface se-5/0/1.0
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
inet  12.0.0.1/30

show interfaces detail (Serial, EIA-530)

user@host> show interfaces se-5/0/1 detail

Physical interface: se-5/0/1, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 41, Generation: 25
  Type: Serial, Link-level type: PPP, MTU: 1504, Maximum speed: 16384kbps
  Device flags : Present Running
  Interface flags: Point-To-Point Internal: 0x4000
  Link flags   : Keepalives
  Hold-times   : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input : 37 (last seen 00:00:06 ago)
    Output: 35 (last sent 00:00:01 ago)
  LCP state: Opened
  CHAP state: Closed
  CoS queues   : 8 supported, 8 maximum usable queues
  Last flapped : 2006-04-26 15:10:18 PDT (00:06:02 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input  bytes  :                  928                   40 bps
    Output bytes  :                 1023                   48 bps
    Input  packets:                   76                    0 pps
    Output packets:                   77                    0 pps

Serial media information:
  Line protocol: eia530
  Resync history:
    Sync loss count: 0
  Data signal:
    Rx Clock: OK
  Control signals:
    Local mode: DTE
    To DCE: DTR: up, RTS: up
    From DCE: CTS: up, DCD: up, DSR: up
    Clocking mode: loop-timed
    Clock rate: 8.0 MHz
    Loopback: none
    Tx clock: non-invert
    Line encoding: nrz

Logical interface se-5/0/1.0 (Index 71) (SNMP ifIndex 45) (Generation 9)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Protocol inet, MTU: 1500, Generation: 15, Route table: 0
Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 12.0.0.0/30, Local: 12.0.0.1, Broadcast: 12.0.0.3,
    Generation: 23

show interfaces extensive (Serial, EIA-530)

user@host> show interfaces se-5/0/1 extensive
Physical interface: se-5/0/1, Enabled, Physical link is Up
Interface index: 144, SNMP ifIndex: 41, Generation: 25
Type: Serial, Link-level type: PPP, MTU: 1504, Maximum speed: 16384kbps
Device flags : Present Running
Interface flags: Point-To-Point Internal: 0x4000
Link flags : Keepalives
Hold-times : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 40 (last seen 00:00:00 ago)
  Output: 37 (last sent 00:00:09 ago)
LCP state: Opened
CHAP state: Closed
Last flapped : 2006-04-26 15:10:18 PDT (00:06:28 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 988 40 bps
  Output bytes : 1088 48 bps
  Input packets: 81 0 pps
  Output packets: 82 0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 2, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0
Serial media information:
  Line protocol: eia530
  Resync history:
    Sync loss count: 0
  Data signal:
    Rx Clock: OK
  Control signals:
    Local mode: DTE
      To DCE: DTR: up, RTS: up
      From DCE: CTS: up, DCD: up, DSR: up
  Clocking mode: loop-timed
  Clock rate: 8.0 MHz
  Loopback: none
  Tx clock: non-invert
  Line encoding: nrz
Packet Forwarding Engine configuration:
  Destination slot: 5, PLP byte: 1 (0x00)
CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>15564800</td>
<td>95</td>
<td>low</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>819200</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface se-5/0/1.0 (Index 71) (SNMP ifIndex 45) (Generation 9)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Protocol inet, MTU: 1500, Generation: 15, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 12.0.0.0/30, Local: 12.0.0.1, Broadcast: 12.0.0.3,
  Generation: 23

Copyright © 2019, Juniper Networks, Inc.
show interfaces (Serial, V.35)

```
user@host> show interfaces se-5/0/0
Physical interface: se-5/0/0, Enabled, Physical link is Down
    Interface index: 150, SNMP ifIndex: 39,
    Type: Serial, Link-level type: PPP, MTU: 1504, Maximum speed: 16384kbps
    Device flags : Present Running Down
    Interface flags: Hardware-Down Point-To-Point Internal: 0x4000
    Link flags   : Loose-NCP
    Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
    Keepalive: Input: 0 (never), Output: 0 (never)
    LCP state: Down
    NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
    mpls: Not-configured
    CHAP state: Closed
    CoS queues   : 8 supported, 8 maximum usable queues
    Last flapped : 2006-04-26 14:51:27 PDT (01:02:23 ago)
    Input rate   : 0 bps (0 pps)
    Output rate  : 0 bps (0 pps)

Logical interface se-5/0/0.0 (Index 73) (SNMP ifIndex 27)
    Flags: Hardware-Down Device-Down Point-To-Point SNMP-Traps
    Encapsulation: PPP
    Protocol inet, MTU: 1500
    Flags: Protocol-Down
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 13.0.0.0/30, Local: 13.0.0.2, Broadcast: 13.0.0.3
```
Physical interface: se-5/0/0, Enabled, Physical link is Down
Interface index: 150, SNMP ifIndex: 39, Generation: 31
Type: Serial, Link-level type: PPP, MTU: 1504, Maximum speed: 16384kbps
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point Internal: 0x4000
Link flags : Loose-NCP
Hold-times : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input: 0 (last seen: never)
  Output: 0 (last sent: never)
LCP state: Down
CHAP state: Closed
CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2006-04-26 14:51:27 PDT (01:04:17 ago)
show interfaces statistics detail (RS 449)

show interfaces se-6/0/0 statistics detail

Related Commands

show interfaces statistics

CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2007-11-28 19:38:36 PST (00:14:06 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 744 0 bps
  Output bytes : 5978 0 bps
  Input packets: 33 0 pps
  Output packets: 129 0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
  Resource errors: 0
Output errors:
  Carrier transitions: 13, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 5 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort 24 24 0
  1 expedited-fo 0 0 0
  2 bulk 0 0 0
  3 assured-forw 105 105 0
  4 voip 0 0 0
Serial media information:
  Line protocol: rs449
Resync history:
  Sync loss count: 0
Data signal:
  Rx Clock: OK
Control signals:
  Local mode: DTE
  To DCE: DTR: up, RTS: up
  From DCE: CTS: up, DCD: up, DSR: up
Clocking mode: internal
Loopback: none
Tx clock: non-invert
Line encoding: nrz
Logical interface se-6/0/0.0 (Index 75) (SNMP ifIndex 69) (Generation 141)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Protocol inet, MTU: 256, Generation: 145, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 11.11.11/24, Local: 11.11.11.2, Broadcast: 11.11.11.255,
    Generation: 157
show interfaces (T1, E1, or DS)

Syntax

show interfaces interface-type
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display status information about the specified T1, E1, or DS interface.

Options

interface-type—On ACX Series, M Series, MX Series, and T Series routers, the T1 interface type is t1-fpc/pic/port, whereas the E1 interface type is e1-fpc/pic/port, and DS interface type is ds-fpc/pic/port:<channel>.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

Related Documentation

- Understanding Interfaces on ACX Series Universal Metro Routers on page 10

List of Sample Output

- show interfaces (T1, IMA Link) on page 1572
- show interfaces (T1, PPP) on page 1573
- show interfaces detail (T1, PPP) on page 1573
- show interfaces extensive (T1 CRC Errors) on page 1574
- show interfaces extensive (T1, PPP) on page 1574
- show interfaces (E1, Frame Relay) on page 1576
- show interfaces detail (E1, Frame Relay) on page 1577
- show interfaces extensive (E1, Frame Relay) on page 1578
- show interfaces (E1, IMA Link) on page 1580
- show interfaces extensive (T1, TDM-CCC-SATOP) on page 1581
- show interfaces extensive (DS, TDM-CCC-CESoPSN) on page 1583

Output Fields

Table 49 on page 1561 lists the output fields for the show interfaces (T1 or E1) 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>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical interface</strong></td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: <strong>Internal</strong> or <strong>External</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (<strong>local</strong> or <strong>remote</strong>).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either <strong>16</strong> or <strong>32</strong>). The default is <strong>16</strong> bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>Physical layer framing format used for the E1 interface on the link: <strong>G704</strong>, <strong>G704-NO-CRC4</strong>, or <strong>Unframed</strong>. The default is <strong>G704</strong>. Physical layer framing format used for the T1 interface on the link: <strong>SF</strong> and <strong>ESF</strong>. The default is <strong>ESF</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>IMA Link alarms</td>
<td>Current active IMA link alarms, including the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• LIF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LODS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RFI-IMA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-Mis-Connected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-Unusable-FE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-Unusable-FE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link Fault</td>
<td></td>
</tr>
<tr>
<td>IMA Link defects</td>
<td>Current active IMA link defects, including the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• LIF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LODS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RFI-IMA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-Mis-Connected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-Unusable-FE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-Unusable-FE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link Fault</td>
<td></td>
</tr>
<tr>
<td>IMA Link state</td>
<td>Current active IMA link status, including the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Line: synchronized or not synchronized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Near end:—Status of near-end receive and transmit links</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx: Usable or Unusable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx: Usable or Unusable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Far end:—Status of far-end receive and transmit links</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx: Usable or Unusable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx: Usable or Unusable</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>IMA link media</td>
<td>IMA Link Media Status, which provides the seconds and count state for the following link media parameters:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• LIF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LODS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Err-ICP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-FC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-FC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Defects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Rx-FC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Tx-FC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-ICP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-Stuff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-ICP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-Stuff</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-SES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-UAS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rx-UUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tx-UUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Rx-SES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Rx-UAS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Rx-UUS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FE-Tx-UUS</td>
<td></td>
</tr>
<tr>
<td>Keepalive settings</td>
<td>(PPP and HDLC) Configured settings for keepalives.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• interval.seconds—The time in seconds between successive keepalive requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• down-count number—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• up-count number—The number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.</td>
<td></td>
</tr>
<tr>
<td>Keepalive statistics</td>
<td>(PPP and HDLC) Information about keepalive packets. When no level of output is specified, the word statistics is not part of the field name and the last seen text is not displayed.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Input—Number of keepalive packets received by PPP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (last seen 00:00:00 ago)—Time since the last keepalive packet was received, in the format hh:mm:ss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (last seen 00:00:00 ago)—Time since the last keepalive packet was sent, in the format hh:mm:ss.</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>LMI settings</td>
<td>(Frame Relay) Settings for Local Management Interface (LMI) which can be either ANSI LMI settings or ITU LMI settings. ANSI LMI settings is the default. The format is (ANSI or ITU) LMI settings: value, value..., xx seconds, where value can be:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n391dte—DTE full status polling interval (1–255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dce—DCE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n392dte—DTE error threshold (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dce—DCE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• n393dte—DTE monitored event count (1–10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t391dte—DTE polling timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• t392dce—DCE polling verification timer (5–30 seconds)</td>
<td></td>
</tr>
<tr>
<td>LMI</td>
<td>(Frame Relay) Local Management Interface (LMI) packet statistics:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Input—Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input: nn (last seen hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output: nn (last sent hh:mm:ss ago).</td>
<td></td>
</tr>
<tr>
<td>DTE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data communications equipment (DCE):</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Enquiries sent—Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiriies sent—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses received—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses received—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
</tr>
<tr>
<td>DCE statistics</td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Enquiries received—Number of enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiriies received—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enquiry responses sent—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Full enquiry responses sent—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 49: T1 or E1 show 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><strong>Common statistics</strong></td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Unknown messages received</strong>—Number of received packets that do not fall into any category.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Asynchronous updates received</strong>—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Out-of-sequence packets received</strong>—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Keepalive responses timedout</strong>—Number of keepalive responses that timed out when no Local Management Interface (LMI) packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td><strong>Nonmatching DCE-end DLCIs</strong></td>
<td>(Frame Relay. Displayed only from the DTE.) Number of DLCIs configured from the DCE.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>LCP state</strong></td>
<td>(PPP) Link Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-received</strong>—Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-sent</strong>—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong>—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not configured</strong>—LCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong>—LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>NCP state</strong></td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-received</strong>—Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-ack-sent</strong>—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Conf-req-sent</strong>—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong>—NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not configured</strong>—NCP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong>—NCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td><strong>CHAP state</strong></td>
<td>(PPP) State of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>- <strong>Chap-Chal-received</strong>—Challenge was received but response is not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Chap-Chal-sent</strong>—Challenge was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Chap-Resp-received</strong>—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Chap-Resp-sent</strong>—Response was sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Down</strong>—CHAP authentication is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Not-configured</strong>—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Opened</strong>—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td><strong>Last flapped</strong></td>
<td>Date, time, and how long ago the interface went from down to up. The format is <strong>Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago)</strong>. For example, <strong>Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)</strong>.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>CoS Queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td>Output rate</td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td>Errors</td>
<td>Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td>Drops</td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Framing errors</td>
<td>Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td>Policed discards</td>
<td>Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td>L3 incompletes</td>
<td>Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td>L2 channel errors</td>
<td>Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td>L2 mismatch timeouts</td>
<td>Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td>HS link CRC errors</td>
<td>Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td>SRAM errors</td>
<td>Number of hardware errors that occurred in the static RAM (SRAM) on the PIC or PIM. If the value of this field increments, the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>Resource errors</td>
<td>Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly, increasing only when the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cable is unplugged, the far-end system is powered down and up, or another</td>
<td></td>
</tr>
<tr>
<td></td>
<td>problem occurs. If the number of carrier transitions increments quickly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(perhaps once every 10 seconds), the cable, the far-end system, or the PIC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>so long that the system automatically purged them. The value in this field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>should never increment. If it does, it is most likely a software bug or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Queued packets</strong>—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Dropped packets</strong>—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>DS1 alarms</strong></td>
<td>E1 media-specific defects that can prevent the interface from passing</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>packets. When a defect persists for a certain amount of time, it is</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>promoted to an alarm. Based on the router configuration, an alarm can</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ring the red or yellow alarm bell on the router, or turn on the red or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>yellow alarm LED on the craft interface. The following lists all possible</td>
<td></td>
</tr>
<tr>
<td></td>
<td>alarms and defects. For complete explanations of most of these alarms and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>defects, see Bellcore Telcordia GR-499-CORE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>AIS</strong>—Alarm indication signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOF</strong>—Loss of frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>LOS</strong>—Loss of signal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>YLW</strong>—Yellow alarm. Indicates errors at the remote site receiver.</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>T1 media or E1 media</td>
<td>Counts of T1 or E1 media-specific errors.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Seconds</strong>—Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the error. State other than <strong>OK</strong> indicates a problem.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The T1 or E1 media-specific error types are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEF</strong>—Severely errored framing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BEE</strong>—Bit error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS</strong>—Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>YELLOW</strong>—Errors at the remote site receiver</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC Major</strong>—Cyclic redundancy check major alarm threshold exceeded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC Minor</strong>—Cyclic redundancy check minor alarm threshold exceeded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BPV</strong>—Bipolar violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>EXZ</strong>—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LCV</strong>—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PCV</strong>—Pulse code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CS</strong>—Carrier state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC</strong>—Cyclic redundancy check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FEBE</strong>—Far-end block error (E1 only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LES</strong>—Line error seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ES</strong>—Errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>BES</strong>—Bursty errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SES</strong>—Severely errored seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SEFS</strong>—Severely errored framing seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>UAS</strong>—Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td>SAToP Configuration</td>
<td>Information about the SAToP configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>payload-size</strong>—Configure the payload size, in bytes (from 32 through 1024 bytes).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>idle-pattern</strong>—An 8-bit hexadecimal pattern to replace TDM data in a lost packet (from 0 through 255).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>jitter-buffer-packets</strong>—Number of packets in the jitter buffer (from 1 through 64 packets).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>jitter-buffer-latency</strong>—Time delay in the jitter buffer (from 1 through 1000 milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>excessive-packet-loss-rate</strong>—Set packet loss options. The options are <strong>groups</strong>, <strong>sample-period</strong>, and <strong>threshold</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>sample-period</strong>—Time required to calculate excessive packet loss rate (from 1000 through 65,535 milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>threshold</strong>—Percentile designating the threshold of excessive packet loss rate (1–100 percent).</td>
<td></td>
</tr>
</tbody>
</table>
### Table 49: T1 or E1 show 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>CESoPSN</td>
<td>Information about the CESoPSN configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• packetization-latency—Time required to create packets (from 1000 through 8000 microseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• idle-pattern—An 8-bit hexadecimal pattern to replace TDM data in a lost packet (from 0 through 255).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• jitter-buffer-packets—Number of packets in the jitter buffer (from 1 through 64 packets).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• jitter-buffer-latency—Time delay in the jitter buffer (from 1 through 1000 milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• excessive-packet-loss-rate—Set packet loss options. The options are sample-period and threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sample-period—Time required to calculate excessive packet loss rate (from 1000 through 65,535 milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• threshold—Percentile designating the threshold of excessive packet loss rate (1–100 percent).</td>
<td></td>
</tr>
<tr>
<td>HDLC configuration</td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Policing bucket—Configured state of the receiving policer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shaping bucket—Configured state of the transmitting shaper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Giant threshold—Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runt threshold—Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeslots—Time slots configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Buildout—(T1 only) Buildout setting: 0-132, 133-265, 266-398, 399-531, or 532-655 feet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeslots—Configured time slots for the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Byte encoding—(T1 only) Byte encoding used: Nx64K or Nx56K.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Line encoding—Line encoding used. For T1, the value can be B8ZS or AMI. For E1, the value is HDB3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data inversion—HDLC data inversion setting: Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Idle cycle flag—Idle cycle flags.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Start end flag—Start and end flag.</td>
<td></td>
</tr>
<tr>
<td>DS1 BERT configuration</td>
<td>BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• BERT time period—Configured total time period that the BERT is to run.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Elapsed—Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Induced error rate—Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Algorithm—Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding Engine configuration</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Destination slot—FPC slot number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PLP byte—Packet Level Protocol byte.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 49: T1 or E1 show 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><strong>Cos information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>• CoS transmit queue</td>
<td>Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth %</td>
<td>Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Bandwidth bps</td>
<td>Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td>• Buffer %</td>
<td>Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td>• Buffer usec</td>
<td>Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td>• Priority</td>
<td>Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td>• Limit</td>
<td>Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical interface</strong></td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Input packets</strong></td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Output packets</strong></td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td><strong>Traffic statistics</strong></td>
<td>(Frame Relay) Number and rate of bytes and packets received and transmitted on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>• Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>• Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Local statistics</strong></td>
<td>(Frame Relay) Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes a while (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</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>Transit statistics</td>
<td>(Frame Relay) Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter normally stabilizes in less than 1 second.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, mfr, or mpls.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Multilink bundle</td>
<td>Interface name for the multilink bundle, if configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics or (Input packets, Output packets). Flags can be one or more of the following:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Active—Set when the link is active and the DTE and DCE are exchanging information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Set when the link is active, but no information is received from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DCE- Unconfigured—Set when the corresponding DLCI in the DCE is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured—Set when the corresponding DLCI in the DCE is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DCE-configured—Displayed when the command is issued from the DTE.</td>
<td></td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Active DLCI—Number of active DLCIs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inactive DLCI—Number of inactive DLCIs.</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: T1 or E1 show 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>CE Info</td>
<td>Information related to the circuit emulation statistics.</td>
<td>extensive</td>
</tr>
<tr>
<td>• CE Tx</td>
<td>Number of transmitted packets and bytes (TDM to PSN flow).</td>
<td></td>
</tr>
<tr>
<td>• CE Rx</td>
<td>Number of received packets and bytes and forward bytes (PSN to TDM flow).</td>
<td></td>
</tr>
<tr>
<td>• CE Rx Forwarded</td>
<td>Number of forwarded bytes.</td>
<td></td>
</tr>
<tr>
<td>• CE Strayed</td>
<td>Number of stray packets.</td>
<td></td>
</tr>
<tr>
<td>• CE Lost</td>
<td>Number of lost packets.</td>
<td></td>
</tr>
<tr>
<td>• CE Malformed</td>
<td>Number of malformed packets</td>
<td></td>
</tr>
<tr>
<td>• CE Misinserted</td>
<td>Number of misinserted packets.</td>
<td></td>
</tr>
<tr>
<td>• CE AIS dropped</td>
<td>Number of dropped bytes due to buffer overrun (PSN to TDM).</td>
<td></td>
</tr>
<tr>
<td>• CE Dropped</td>
<td>Number of dropped packets during resynchronization</td>
<td></td>
</tr>
<tr>
<td>• CE Overrun Events</td>
<td>Number of overrun events.</td>
<td></td>
</tr>
<tr>
<td>• CE Underrun Events</td>
<td>Number of underrun events.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show interfaces (T1, IMA Link)

user@host> show interfaces t1-1/0/0

IMA Link alarms : None
IMA Link defects : LIF, LOSS
IMA Link state:
  Line     : Not synchronized
  Near end : Rx: Unusable, Tx: Usable
  Far  end : Rx: Unusable, Tx: Usable
IMA link media:

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIF</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>LOSS</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Err-ICP</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Rx-FC</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Tx-FC</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>FE-Defects</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Rx-FC</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Tx-FC</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx-ICP</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx-Stuff</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx-ICP</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx-Stuff</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx-SES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx-UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx-UUS</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tx-UUS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Rx-SES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Rx-UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Rx-UUS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FE-Tx-UUS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show interfaces (T1, PPP)

user@host> show interfaces t1-1/1/0

Physical interface: t1-1/1/0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 45
Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: T1,
Loopback: None, FCS: 16, Framing: ESF
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 0 (never), Output: 0 (never)
LCP state: Opened
NCP state: Opened
CHAP state: Opened
CoS queues : 4 supported, 4 in use
Last flapped : 2005-12-05 08:43:06 PST (02:13:35 ago)
Input rate : 0 bps (0 pps)
Output rate : 72 bps (0 pps)
DS1 alarms : None
DS1 defects : None

Logical interface t1-1/1/0.0 (Index 66) (SNMP ifIndex 51)
Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 1500
Flags: Protocol-Down
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
   Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255

show interfaces detail (T1, PPP)

user@host> show interfaces t1-1/1/0 detail

Physical interface: t1-1/1/0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 45, Generation: 32
Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: T1,
Loopback: None, FCS: 16, Framing: ESF
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Hold-times : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
   Input : 0 (last seen: never)
   Output: 0 (last sent: never)
LCP state: Opened
NCP state: Opened
CHAP state: Opened
CoS queues : 4 supported, 4 in use
Last flapped : 2005-12-05 08:43:06 PST (02:13:52 ago)
Statistics last cleared: Never
Traffic statistics:
   Input bytes : 0 0 bps
   Output bytes : 798 0 bps
   Input packets: 0 0 pps
   Output packets: 42 0 pps
Queue counters: Queued packets Transmitted packets Dropped packets
Interfaces Fundamentals for Routing Devices

0 best-effort                    0                    0                    0
1 expedited-fo                   0                    0                    0
2 assured-forw                   0                    0                    0
3 network-cont                    40                   40                    0

DS1    alarms   : None
DS1    defects  : None
DS1 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^15 - 1
Logical interface t1-1/1/0.0 (Index 66) (SNMP ifIndex 51) (Generation 5)
  Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol inet, MTU: 1500, Generation: 14, Route table: 0
  Flags: Protocol-Down
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255,
  Generation: 18

show interfaces extensive (T1 CRC Errors)

```bash
user@host> show interfaces t1-3/2/0:1:1 extensive
```
Physical interface: t1-3/2/0:1:1, Enabled, Physical link is Down
  Interface index: 179, SNMP ifIndex: 79, Generation: 180
  :
  DS1    alarms   : AIS, LOF, CRC Major, CRC Minor
  DS1    defects  : AIS, LOF, CRC Major, CRC Minor
  T1    media:            Seconds  Count  State
         SEF             1        1  OK
         BEE             1        1  OK
         AIS            1128       1  Defect Active
         LOF            1128       1  Defect Active
         LOS             0        0  OK
         YELLOW         0        0  OK
         CRC Major      154       1  Defect Active
         CRC Minor      154       1  Defect Active
         BPV             0        0
         EXZ             0        0
         LCV             0        0
         PCV             0        0
         CS              0        0
         CRC            154      15400
  ...
```

show interfaces extensive (T1, PPP)

```bash
user@host> show interfaces t1-1/1/0 extensive
```
Physical interface: t1-1/1/0, Enabled, Physical link is Up
  Interface index: 149, SNMP ifIndex: 45, Generation: 32
  Link-level type: PPP, MTU: 1504, Clocking: Internal, Speed: T1,
  Loopback: None, FCS: 16, Framing: ESF
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives
Hold-times : Up 0 ms, Down 0 ms
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 0 (last seen: never)
  Output: 0 (last sent: never)
LCP state: Down
NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Closed
CoS queues : 4 supported, 4 in use
Last flapped : 2005-12-05 08:43:06 PST (02:13:54 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 0 0 bps
  Output bytes : 817 72 bps
  Input packets: 0 0 pps
  Output packets: 43 0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
  HS link CRC errors: 0, SRAM errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
  Resource errors: 0
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort 0 0 0
  1 expedited-fo 0 0 0
  2 assured-forw 0 0 0
  3 network-cont 42 42 0
DS1 alarms : None
DS1 defects : None
T1 media: Seconds Count State
  SEF 1 1 OK
  BEE 0 0 OK
  AIS 0 0 OK
  LOF 1 1 OK
  LOS 0 0 OK
  YELLOW 1 1 OK
  BPV 1 1
  EXZ 1 1
  LCV 1 65535
  PCV 1 1023
  CS 0 0
  LES 1
  ES 1
  SES 1
  SEFS 1
  BES 0
  UAS 0
HDLC configuration:
Policing bucket: Disabled
Shaping bucket : Disabled
Giant threshold: 1514, Runt threshold: 3
Timeslots : All active
Line encoding: B8ZS
Buildout : 0 to 132 feet
Byte encoding: Nx64K, Data inversion: Disabled, Idle cycle flag: flags,
Start end flag: shared
DS1 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^15 - 1
Packet Forwarding Engine configuration:
Destination slot: 1, PLP byte: 1 (0x00)
CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer usec</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>1459200</td>
<td>95</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>76800</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface t1-1/1/0.0 (Index 66) (SNMP ifIndex 51) (Generation 5)
Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 1500, Generation: 14, Route table: 0
Flags: Protocol-Down
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast:
  198.51.100.255,
  Generation: 18

show interfaces (E1, Frame Relay)

user@host> show interfaces e1-3/0/0

Physical interface: e1-3/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 37
Link-level type: Frame-Relay, MTU: 1504, Clocking: Internal, Speed: E1,
Loopback: None, FCS: 16, Framing: G704
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps 16384
Link flags : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 0 (never), Output: 11 (00:00:05 ago)
DTE statistics:
  Enquiries sent : 10
  Full enquiries sent : 1
  Enquiry responses received : 0
  Full enquiry responses received : 0
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 1
CoS queues : 8 supported
Last flapped : 2005-11-30 14:50:34 PST (4d 20:33 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
DS1 alarms : None
DS1 defects : None
Logical interface e1-3/0/0.0 (Index 72) (SNMP ifIndex 32)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Input packets : 0
Output packets: 0
Protocol inet, MTU: 1500
  Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.1.3/24, Local: 10.1.3.1, Broadcast: 10.1.3.255
DLCI 100
  Flags: Down, DCE-Unconfigured
  Total down time: 00:01:13 sec, Last down: 00:01:13 ago
Input packets : 0
Output packets: 0
DLCI statistics:
  Active DLCI :0 Inactive DLCI :1

show interfaces detail (E1, Frame Relay)

user@host> show interfaces e1-3/0/0 detail

Physical interface: e1-3/0/0, Enabled, Physical link is Up
  Interface index: 146, SNMP ifIndex: 37, Generation: 69
  Link-level type: Frame-Relay, MTU: 1504, Clocking: Internal, Speed: E1,
  Loopback: None, FCS: 16, Framing: G704
  Device flags : Present Running
  Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps 16384
  Link flags : Keepalives DTE
  Hold-times : Up 0 ms, Down 0 ms
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI statistics:
    Input : 0 (last seen: never)
    Output: 12 (last sent 00:00:02 ago)
  DTE statistics:
    Enquiries sent : 10
    Full enquiries sent : 2
    Enquiry responses received : 0
    Full enquiry responses received : 0
  DCE statistics:
    Enquiries received : 0
    Full enquiries received : 0
    Enquiry responses sent : 0
    Full enquiry responses sent : 0
  Common statistics:
    Unknown messages received : 0
    Asynchronous updates received : 0
    Out-of-sequence packets received : 0
    Keepalive responses timedout : 1
  CoS queues : 8 supported
  Last flapped : 2005-11-30 14:50:34 PST (4d 20:33 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 225 56 bps
    Input packets: 0 0 pps
    Output packets: 15 0 pps
  Queue counters: 0 limited 0 Transmitted packets 0 Dropped packets
  0 expedited-fo 0
  1
show interfaces extensive (E1, Frame Relay)

show interfaces e1-3/0/0 extensive

Physical interface: e1-3/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 37, Generation: 69
Link-level type: Frame-Relay, MTU: 1504, Clocking: Internal, Speed: E1,
Loopback: None, FCS: 16, Framing: G704
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps 16384
Link flags : Keepalives DTE
Hold-times : Up 0 ms, Down 0 ms
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI statistics:
Input : 0 (last seen: never)
Output: 12 (last sent 00:00:05 ago)
DTE statistics:
Enquiries sent : 10

showinterfacesextensive(E1,FrameRelay)
Full enquiries sent : 2
Enquiry responses received : 0
Full enquiry responses received : 0
DCE statistics:
Enquiries received : 0
Full enquiries received : 0
Enquiry responses sent : 0
Full enquiry responses sent : 0
Common statistics:
Unknown messages received : 0
Asynchronous updates received : 0
Out-of-sequence packets received : 0
Keepalive responses timedout : 1
CoS queues : 8 supported
Last flapped : 2005-11-30 14:50:34 PST (4d 20:33 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 225 0 bps
Input packets: 0 0 pps
Output packets: 15 0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
HS link CRC errors: 0, SRAM errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 17, Errors: 0, Drops: 0, Aged packets: 0,
MTU errors: 0, Resource errors: 0
Queue counters:
  Queued packets Transmitted packets Dropped packets
0 limited 0 0 0
1 expedited-fo 0 0 0
2 real-plus 0 0 0
3 network-cont 15 15 0
DS1 alarms : None
DS1 defects : None
E1 media: Seconds Count State
SEF 0 0 OK
BEE 5 5 OK
AIS 0 0 OK
LOF 245 15 OK
LOS 245 4 OK
YELLOW 0 11 OK
BPV 0 0
EXZ 9 9
LCV 0 0
PCV 0 0
CS 0 0
FEBE 0 0
LES 0
ES 0
SES 0
SEFS 0
BES 0
UAS 271
HDLC configuration:
Policing bucket: Disabled
Shaping bucket : Disabled
Giant threshold: 1506, Runt threshold: 0
Timeslots : All active
Line encoding: HDB3, Data inversion: Disabled, Idle cycle flag: flags,
Start end flag: shared
DS1 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 10e-0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)
Packet Forwarding Engine configuration:
Destination slot: 3, PLP byte: 1 (0x00)
CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 limited</td>
<td>95</td>
<td>1945600</td>
<td>95</td>
<td>low</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>102400</td>
<td>5</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface e1-3/0/0.0 (Index 72) (SNMP ifIndex 32) (Generation 26)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: 1500, Generation: 32, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.1.3/24, Local: 10.1.3.1, Broadcast: 10.1.3.255,
Generation: 42
DLCI 100
Flags: Down, DCE-Unconfigured
Total down time: 00:01:21 sec, Last down: 00:01:21 ago
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
DLCI statistics:
Active DLCI :0 Inactive DLCI :1
show interfaces extensive (T1, TDM-CCC-SATOP)

user@host> show interfaces t1-1/0/0:1:1 extensive

Physical interface: t1-1/0/0:1:1, Enabled, Physical link is Down
  Interface index: 153, SNMP ifIndex: 579, Generation: 817
  Link-level type: TDM-CCC-SATOP, MTU: 1504, Clocking: Internal, Speed: T1,
  Loopback: None, FCS: 16, Framing: ESF,
  Parent: coc1-1/0/0:1 Interface index 152
  Device flags : Present Running Down
  Interface flags: Hardware-Down Point-To-Point SNMP-Traps Internal: 0x0
  Link flags : None
  Hold-times : Up 0 ms, Down 0 ms
  CoS queues : 8 supported, 8 maximum usable queues
  Last flapped : 2012-10-28 02:12:40 PDT (22:32:13 ago)
  Statistics last cleared: 2012-10-29 00:44:52 PDT (00:00:01 ago)
  Egress queues: 8 supported, 4 in use

Queue counters:           Queued packets Transmitted packets Dropped packets
  0 best-effort            0                    0                    0
  1 expedited-fo           0                    0                    0
  2 assured-forward        0                    0                    0
  3 network-control        0                    0                    0

Queue number:  Mapped forwarding classes
  0 best-effort
  1 expedited-forwarding
  2 assured-forwarding
  3 network-control

DS1 alarms : None
DS1 defects : None

T1 media:
  Seconds  Count  State
  SEF       0       0    OK
  BEE       0       0    OK
  AIS       0       0    OK
<table>
<thead>
<tr>
<th>Metric</th>
<th>Count</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOF</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>YELLOW</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>CRC Major</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>CRC Minor</td>
<td>0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>BPV</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXZ</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCV</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCV</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRC</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEFS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SAToP configuration:**
- **Payload size:** 192
- **Idle pattern:** 0xFF
- **Octet aligned:** Disabled
- **Jitter buffer:** packets: 8, latency: 7 ms, auto adjust: Disabled
- **Excessive packet loss rate:** sample period: 10000 ms, threshold: 30%

**DS1 BERT configuration:**
- **BERT time period:** 10 seconds, Elapsed: 0 seconds
- **Induced Error rate:** 0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)

**SONET alarms:** None
**SONET defects:** AIS-V, RDI-V

**SONET vt:**
- **BIP-BIP2** 0 0
- **REI-V** 0 0
- **LOP-V** 0 0 OK
- **AIS-V** 2 0 Defect Active
- **RDI-V** 2 0 Defect Active
- **UNEQ-V** 0 0 OK
- **PLM-V** 0 0 OK
- **ES-V** 0
- **SES-V** 0
- **UAS-V** 0
- **ES-VFE** 0
- **SES-VFE** 0
- **UAS-VFE** 0

**Received SONET overhead:**
- **V5** : 0x07
- **V5(cmp)** : 0x02

**Transmitted SONET overhead:**
- **V5** : 0x02

**Packet Forwarding Engine configuration:**
- **Destination slot:** 1

**CoS information:**
- **Direction:** Output
- **CoS transmit queue**

<table>
<thead>
<tr>
<th>Limit</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>1459200</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>76800</td>
</tr>
</tbody>
</table>

**Logical interface tl-1/0/0:1:1.0 (Index 69) (SNMP ifIndex 580) (Generation 525)**
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: TDM-CCC-SATOP

CE info Packets Bytes Count
CE Tx 1005 192960
CE Rx 1004 192768
CE Rx Forwarded 0
CE Strayed 0
CE Lost 0
CE Malformed 0
CE Misinserted 0
CE AIS dropped 0
CE Dropped 1005 192960
CE Overrun Events 0
CE Underrun Events 0

Protocol ccc, MTU: 1504, Generation: 814, Route table: 0
Flags: Is-Primary

show interfaces extensive (DS, TDM-CCC-CESoPSN)

user@host> show interfaces ds-1/0/0:1:1:1 extensive

Physical interface: ds-1/0/0:1:1:1, Enabled, Physical link is Down
Interface index: 154, SNMP ifIndex: 597, Generation: 819
Device flags : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps Internal: 0x0
Link flags : None
Hold-times : Up 0 ms, Down 0 ms
CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2012-10-29 00:49:03 PDT (00:00:35 ago)
Statistics last cleared: Never
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 0 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
CESoPSN configuration:
Packetization latency: 1000 us
Idle pattern: 0xFF
Jitter buffer: packets: 8, latency: 8 ms, auto adjust: Disabled
Excessive packet loss rate: sample period: 10000 ms, threshold: 30%
DS0 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Induced Error rate: 0, Algorithm: 2^15 - 1, 0.151, Pseudorandom (9)
Packet Forwarding Engine configuration:
Destination slot: 1
CoS information:
Direction : Output
<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>%</td>
<td>bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>1459200</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>76800</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logical interface ds-1/0/0:1:1:1.0 (Index 69) (SNMP ifIndex 598) (Generation 549)

Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: TDM-CCC-CESoPSN

CE info

<table>
<thead>
<tr>
<th>CE info</th>
<th>Packets</th>
<th>Bytes</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE Tx</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Rx</td>
<td>35712</td>
<td>6856704</td>
<td>0</td>
</tr>
<tr>
<td>CE Rx Forwarded</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CE Strayed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Lost</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Malformed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Misinserted</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE AIS dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Dropped</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Overrun Events</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE Underrun Events</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Protocol ccc, MTU: 1504, Generation: 857, Route table: 0

Flags: Is-Primary
show interfaces (T3 or E3)

Syntax

```
show interfaces interface-type
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>
```

Release Information
Command introduced before Junos OS Release 7.4.

Description
Display status information about the specified T3 or E3 interface.

Options
- `interface-type`—On M Series and T Series routers, the T3 interface type is `t3-fpc/pic/port`, whereas the E3 interface type is `e3-fpc/pic/port`.

- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.

- `descriptions`—(Optional) Display interface description strings.

- `media`—(Optional) Display media-specific information about network interfaces.

- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.


Required Privilege
view

List of Sample Output
- `show interfaces (T3, PPP)` on page 1594
- `show interfaces detail (T3, PPP)` on page 1595
- `show interfaces extensive (T3, PPP)` on page 1596
- `show interfaces (E3, Frame Relay)` on page 1597
- `show interfaces detail (E3, Frame Relay)` on page 1598
- `show interfaces extensive (E3, Frame Relay)` on page 1600

Output Fields
Table 50 on page 1585 lists the output fields for the `show interfaces` (T3 or E3) command. Output fields are listed in the approximate order in which they appear.

Table 50: T3 or E3 show interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 50: T3 or E3 show 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>Interface index</td>
<td>Physical interface's index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source. It can be Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loopback</td>
<td>Whether loopback is enabled and the type of loopback (local or remote).</td>
<td>All levels</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame check sequence on the interface (either 16 or 32). The default is 16 bits.</td>
<td>All levels</td>
</tr>
<tr>
<td>Mode</td>
<td>(T3 only) Whether C-bit parity mode or M13 mode is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Long buildout</td>
<td>(T3 only) Buildout setting: less than 255 feet (68 meters) or greater than 255 feet and shorter than 450 feet (137 meters).</td>
<td>All levels</td>
</tr>
<tr>
<td>Framing</td>
<td>(E3 only) Physical layer framing format used on the link. It can be G751 or Unframed. The default is G751.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Keepalive settings (PPP and HDLC) Configured settings for keepalives.

- **interval seconds**—Time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds.
- **down-count number**—Number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3.
- **up-count number**—Number of keepalive packets a destination must receive to change a link’s status from down to up. The range is 1 through 255, with a default of 1.
### Table 50: T3 or E3 show 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><strong>Keepalive statistics</strong> or <strong>Keepalive</strong></td>
<td>(PPP and HDLC) Information about keepalive packets.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• <strong>Input</strong>—Number of keepalive packets received by PPP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was received, in the format <em>hh:mm:ss</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output</strong>—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <em>(last seen 00:00:00 ago)</em>—Time since the last keepalive packet was sent, in the format <em>hh:mm:ss</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LMI settings</strong></td>
<td>(Frame Relay) Local Management Interface (LMI) settings (ANSI or ITU). ANSI LMI settings is the default. The format is LMI settings: value, value... xx seconds, where value can be:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• n391dte—DTE full status polling interval (1–255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• n392dce—DCE error threshold (1–10)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• n392dte—DCE error threshold (1–10)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• n393dce—DCE monitored event count (1–10)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• n393dte—DTE monitored event count (1–10)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• t391dte—DTE polling timer (5–30 seconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• t392dce—DCE polling verification timer (5–30 seconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LMI</strong></td>
<td>(Frame Relay) LMI statistics:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• <strong>Input</strong>—Number of packets coming in on the interface (nn) and how much time has passed since the last packet arrived. The format is Input: <em>nn</em> (last seen <em>hh:mm:ss</em> ago).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Output</strong>—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent. The format is Output: <em>nn</em> (last sent <em>hh:mm:ss</em> ago).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DTE statistics</strong></td>
<td>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data communications equipment (DCE):</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• <strong>Enquiries sent</strong>—Number of link status enquiries sent from the DTE to the DCE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Full enquiries sent</strong>—Number of full enquiries sent from the DTE to the DCE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Enquiry responses received</strong>—Number of enquiry responses received by the DTE from the DCE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Full enquiry responses received</strong>—Number of full enquiry responses sent from the DTE to the DCE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DCE statistics</strong></td>
<td>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>• <strong>Enquiries received</strong>—Number of enquiries received by the DCE from the DTE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Full enquiries received</strong>—Number of full enquiries received by the DCE from the DTE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Enquiry responses sent</strong>—Number of enquiry responses sent from the DCE to the DTE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Full enquiry responses sent</strong>—Number of full enquiry responses sent from the DCE to the DTE.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 50: T3 or E3 show 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>Common statistics</td>
<td>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Unknown messages received—Number of received packets that do not fall into any category.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Asynchronous updates received—Number of link status peer changes received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Out-of-sequence packets received—Number of packets for which the sequence of the packets received is different from the expected sequence.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Keepalive responses timed out—Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.)</td>
<td></td>
</tr>
<tr>
<td>Nonmatching DCE-end DLCIs</td>
<td>(Frame Relay. Displayed only from the DTE.) Number of DLCIs configured from the DCE.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LCP state</td>
<td>(PPP) Link Control Protocol state.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Conf-ack-received—Acknowledgement was received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Conf-ack-sent—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Conf-req-sent—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—LCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Opened—LCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td>NCP state</td>
<td>(PPP) Network Control Protocol state.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Conf-ack-received—Acknowledgement was received.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Conf-ack-sent—Acknowledgement was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Conf-req-sent—Request was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—NCP negotiation is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Opened—NCP negotiation is successful.</td>
<td></td>
</tr>
<tr>
<td>CHAP state</td>
<td>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Chap-Resp-received—Response received for the challenge sent, but CHAP not yet moved into the Success state. (Most likely with RADIUS authentication.)</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Chap-Resp-sent—Response sent for the challenge received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chap-Chal-sent—Challenge sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chap-Chal-received—Challenge received but response not yet sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—CHAP authentication is incomplete (not yet completed or has failed).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not-configured—CHAP is not configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Opened—CHAP authentication was successful.</td>
<td></td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minutes:second timezone (year-month-day hour:minutes:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>none</td>
</tr>
</tbody>
</table>
### Table 50: T3 or E3 show 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>Input rate</td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>None specified</td>
</tr>
<tr>
<td>Output rate</td>
<td>Output rate in bps and pps.</td>
<td>None specified</td>
</tr>
<tr>
<td>Statistics last</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>cleared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>whose meaning might not be obvious:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the input queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Framing errors—Number of packets received with an invalid frame checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runtst—(T3 only) Number of frames received that are smaller than the runt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Giants—(T3 only) Number of frames received that are larger than the giant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bucket Drops—Drops resulting from the traffic load exceeding the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transmit/receive leaky bucket configuration. The default is off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policed discards—Number of frames that the incoming packet match code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discarded because they were not recognized or not of interest. Usually, this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L3 incompletes—Number of incoming packets discarded because they failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L2 channel errors—Number of times the software did not find a valid logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L2 mismatch timeouts—Number of malformed or short packets that caused</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• H5 link CRC errors—Number of errors on the high-speed links between the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASICS responsible for handling the router interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SRAM errors—Number of hardware errors that occurred in the static RAM (SRAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on the PIC or PIM. If the value of this field increments, the PIC or PIM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 50: T3 or E3 show 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><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Queue counters</strong></td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued packets</strong>—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dropped packets</strong>—Number of packets dropped by the ASIC's RED mechanism.</td>
<td></td>
</tr>
<tr>
<td><strong>Active alarms</strong></td>
<td>E3 media-specific defects that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>AIS</strong>—Alarm indication signal</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>EXZ</strong>—Excessive zeros</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FERF</strong>—Far-end receive failures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>IDL</strong>—Idle code detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LCD</strong>—Loss of cell delineation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LCV</strong>—Line code violation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOF</strong>—Loss of frame</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LOS</strong>—Loss of signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLL</strong>—Phase-locked loop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>YLW</strong>—Remote defect indication</td>
<td></td>
</tr>
</tbody>
</table>
Table 50: T3 or E3 show 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><strong>DS3 media or E3  media</strong></td>
<td>Counts of DS3 (T3) or E3 media-specific errors.</td>
<td>extensive</td>
</tr>
<tr>
<td>• <strong>Seconds</strong></td>
<td>Number of seconds the defect has been active.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Count</strong></td>
<td>Number of times that the defect has gone from inactive to active.</td>
<td></td>
</tr>
<tr>
<td>• <strong>State</strong></td>
<td>State of the error. State other than OK indicates a problem.</td>
<td></td>
</tr>
<tr>
<td>The DS3 or E3 media-specific error types can be:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>PLLock</strong></td>
<td>Phase-locked loop out of lock</td>
<td></td>
</tr>
<tr>
<td>• <strong>Reframing</strong></td>
<td>Frame alignment recovery time</td>
<td></td>
</tr>
<tr>
<td>• <strong>AIS</strong></td>
<td>Alarm indication signal</td>
<td></td>
</tr>
<tr>
<td>• <strong>LOF</strong></td>
<td>Loss of frame</td>
<td></td>
</tr>
<tr>
<td>• <strong>LOS</strong></td>
<td>Loss of signal</td>
<td></td>
</tr>
<tr>
<td>• <strong>IDLE</strong></td>
<td>Idle code detected</td>
<td></td>
</tr>
<tr>
<td>• <strong>YELLOW</strong></td>
<td>Errors at the remote site receiver</td>
<td></td>
</tr>
<tr>
<td>• <strong>BPV</strong></td>
<td>Bipolar violation</td>
<td></td>
</tr>
<tr>
<td>• <strong>EXZ</strong></td>
<td>Excessive zeros</td>
<td></td>
</tr>
<tr>
<td>• <strong>LCV</strong></td>
<td>Line code violation</td>
<td></td>
</tr>
<tr>
<td>• <strong>PCV</strong></td>
<td>(DS3 only) Pulse code violation</td>
<td></td>
</tr>
<tr>
<td>• <strong>CCV</strong></td>
<td>(DS3 only) C-bit coding violation</td>
<td></td>
</tr>
<tr>
<td>• <strong>FEBE</strong></td>
<td>(DS3 only) Far-end block error</td>
<td></td>
</tr>
<tr>
<td>• <strong>LES</strong></td>
<td>Line error seconds</td>
<td></td>
</tr>
<tr>
<td>• <strong>PES</strong></td>
<td>(DS3 only) P-bit errored seconds</td>
<td></td>
</tr>
<tr>
<td>• <strong>PSES</strong></td>
<td>(DS3 only) P-bit errored seconds (section)</td>
<td></td>
</tr>
<tr>
<td>• <strong>CE5</strong></td>
<td>(DS3 only) C-bit errored seconds</td>
<td></td>
</tr>
<tr>
<td>• <strong>CSES</strong></td>
<td>(DS3 only) C-bit severely errored seconds</td>
<td></td>
</tr>
<tr>
<td>• <strong>SEFS</strong></td>
<td>Severely errored framing seconds</td>
<td></td>
</tr>
<tr>
<td>• <strong>UAS</strong></td>
<td>Unavailable seconds</td>
<td></td>
</tr>
<tr>
<td><strong>HDLC configuration</strong></td>
<td>Information about the HDLC configuration.</td>
<td>extensive</td>
</tr>
<tr>
<td>• <strong>Policing bucket</strong></td>
<td>Configured state of the receiving policer.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Shaping bucket</strong></td>
<td>Configured state of the transmitting shaper.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Giant threshold</strong></td>
<td>Giant threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Runt threshold</strong></td>
<td>Runt threshold programmed into the hardware.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Idle cycle flag</strong></td>
<td>Idle cycle flags.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Start end flag</strong></td>
<td>Start and end flag.</td>
<td></td>
</tr>
</tbody>
</table>
Table 50: T3 or E3 show 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><strong>DSU configuration</strong></td>
<td>Information about the DSU configuration. The last three lines (Bit count, Error bit count, and LOS information) are displayed only if a BERT has ever been run on the interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Compatibility mod</strong>—CSU/DSU compatibility mode: None, Larscom, Kentrox, or Digital-Link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Scrambling</strong>—Payload scrambling: Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Subrate</strong>—Configured subrate setting. Applies only when Digital-Link compatibility mode is used. The subrate can be Disabled or display units in Kbps.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FEAC loopbac</strong>—(T3) Whether a far-end alarm and control (FEAC) loopback is Active or Inactive. This feature is used to send alarm or status information from the far-end terminal back to the near-end terminal and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Response</strong>—Whether the FEAC signal is Enabled or Disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Count</strong>—Number of FEAC loopbacks.</td>
<td></td>
</tr>
<tr>
<td><strong>DS3 (or E3) BERT configuration</strong></td>
<td>BERT (bit error rate test) checks the quality of the line. This output appears only when a BERT is run on the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <strong>BERT time period</strong>—Configured total time period that the BERT is to run.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Elapsed</strong>—Actual time elapsed since the start of the BERT (in seconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Induced error rate</strong>—Configured rate at which the bit errors are induced in the BERT pattern.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Algorithm</strong>—Type of algorithm selected for the BERT.</td>
<td></td>
</tr>
<tr>
<td><strong>Packet Forwarding Engine configuration</strong></td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination slot</strong>—FPC slot number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PLP byte</strong>—Packet Level Protocol byte.</td>
<td></td>
</tr>
<tr>
<td><strong>CoS information</strong></td>
<td>Information about the CoS queue for the physical interface.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>CoS transmit queue</strong>—Queue number and its associated user-configured forwarding class name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth %</strong>—Percentage of bandwidth allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bandwidth bps</strong>—Bandwidth allocated to the queue (in bps).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer %</strong>—Percentage of buffer space allocated to the queue.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Buffer usec</strong>—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Priority</strong>—Queue priority: low or high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Limit</strong>—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available.</td>
<td></td>
</tr>
<tr>
<td><strong>Logical Interface</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 50: T3 or E3 show 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>Logical interface</td>
<td>Name of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP interface</td>
<td>Logical interface SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the logical interface.</td>
<td>None specified</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>(Frame Relay) Number and rate of bytes and packets received and transmitted on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>(Frame Relay) Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>(Frame Relay) Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter normally stabilizes in less than 1 second.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as <em>iso</em>, <em>inet6</em>, <em>mlfr</em>, or <em>mpls</em>.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Multilink bundle</td>
<td>(Multilink) Interface name for the multilink bundle.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
### Table 50: T3 or E3 show 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>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI</td>
<td>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics (or Input packets, Output packets). Flags is one or more of the following:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>DLCI statistics</td>
<td>(Frame Relay) Data-link connection identifier (DLCI) statistics.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Active—Set when the link is active and the DTE and DCE are exchanging information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Set when the link is active, but no information is received from the DCE.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DCE Unconfigured—Set when the corresponding DLCI in the DCE is not configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configured—Set when the corresponding DLCI in the DCE is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DCE-configured—Displayed when the command is issued from the DTE.</td>
<td></td>
</tr>
</tbody>
</table>

#### Sample Output

**show interfaces (T3, PPP)**

```
user@host> show interfaces t3-0/2/0

Physical interface: t3-0/2/0, Enabled, Physical link is Up
  Interface index: 139, SNMP ifIndex: 35
  Link-level type: PPP, MTU: 4474, Clocking: Internal, Speed: T3,
  Loopback: None, FCS: 16, Mode: C/Bit parity,
  Long buildout: Shorter than 255 feet
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 0 (never)
  LCP state: Down
  NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Closed
  CoS queues     : 4 supported, 4 in use
```
<table>
<thead>
<tr>
<th>Last flapped</th>
<th>2005-12-05 08:43:06 PST (02:18:40 ago)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input rate</td>
<td>0 bps (0 pps)</td>
</tr>
<tr>
<td>Output rate</td>
<td>72 bps (0 pps)</td>
</tr>
<tr>
<td>Active alarms</td>
<td>None</td>
</tr>
<tr>
<td>Active defects</td>
<td>None</td>
</tr>
<tr>
<td>DS3 BERT configuration:</td>
<td></td>
</tr>
<tr>
<td>BERT time period</td>
<td>10 seconds, Elapsed: 0 seconds</td>
</tr>
<tr>
<td>Algorithm</td>
<td>$2^{15} - 1$, 0.151, Pseudorandom (9), Induced error rate: $10^{-0}$</td>
</tr>
</tbody>
</table>

**Logical interface t3-0/2/0.0 (Index 66) (SNMP ifIndex 54)**

- Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
- Protocol inet, MTU: 4470
- Flags: Protocol-Down
- Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
- Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255

```plaintext
show interfaces detail (T3, PPP)
```

```plaintext
user@host> show interfaces t3-0/2/0 detail

Physical interface: t3-0/2/0, Enabled, Physical link is Up
- Interface index: 139, SNMP ifIndex: 35, Generation: 22
- Link-level type: PPP, MTU: 4474, Clocking: Internal, Speed: T3,
- Loopback: None, FCS: 16, Mode: C/Bit parity,
- Long buildout: Shorter than 255 feet
- Device flags : Present Running
- Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
- Link flags : Keepalives
- Hold-times : Up 0 ms, Down 0 ms
- Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
- Keepalive statistics:
  - Input: 0 (last seen: never)
  - Output: 0 (last sent: never)
- LCP state: Down
- CHAP state: Closed
- CoS queues : 4 supported, 4 in use
- Last flapped : 2005-12-05 08:43:06 PST (02:18:45 ago)
- Statistics last cleared: Never

Traffic statistics:

<table>
<thead>
<tr>
<th>Input bytes</th>
<th>0</th>
<th>0 bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output bytes</td>
<td>152</td>
<td>0 bps</td>
</tr>
<tr>
<td>Input packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>Output packets</td>
<td>8</td>
<td>0 pps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms : None
Active defects : None
DS3 BERT configuration:
- BERT time period: 10 seconds, Elapsed: 0 seconds
Interfaces Fundamentals for Routing Devices

Algorithm: $2^{15} - 1$, 0.151, Pseudorandom (9), Induced error rate: 10e-0

Logical interface t3-0/2/0.0 (Index 66) (SNMP ifIndex 54) (Generation 8)
  Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol inet, MTU: 4470, Generation: 17, Route table: 0
  Flags: Protocol-Down
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast:
  198.51.100.255,
  Generation: 24

show interfaces extensive (T3, PPP)

user@host> show interfaces t3-0/2/0 extensive

Physical interface: t3-0/2/0, Enabled, Physical link is Up
  Interface index: 139, SNMP ifIndex: 35, Generation: 22
  Link-level type: PPP, MTU: 4474, Clocking: Internal, Speed: T3,
  Loopback: None, FCS: 16, Mode: C/Bit parity,
  Long buildout: Shorter than 255 feet
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : Keepalives
  Hold-times : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input : 0 (last seen: never)
    Output: 0 (last sent: never)
  LCP state: Down
  NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Closed
  CoS queues : 4 supported, 4 in use
  Last flapped : 2005-12-05 08:43:06 PST (02:18:47 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 171 72 bps
    Input packets: 0 0 pps
    Output packets: 9 0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Bucket drops: 0, Policed discards: 0, L3 incompletes: 0,
    L2 channel errors: 0, L2 mismatch timeouts: 0, HS link CRC errors: 0,
    SRAM errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
    Resource errors: 0
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 best-effort 0 0 0
    1 expedited-fo 0 0 0
    2 assured-forw 0 0 0
    3 network-cont 7 7 0
  Active alarms : None
Active defects: None

<table>
<thead>
<tr>
<th>DS3 media</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLL Lock</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>Reframing</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>AIS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOF</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>IDLE</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>YELLOW</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>BPV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>EXZ</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LCV</td>
<td>1</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>PCV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CCV</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>FEBE</td>
<td>1</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>LES</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSES</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEFS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HDLC configuration:
Policing bucket: Disabled
Shaping bucket: Disabled
Giant threshold: 4484, Runt threshold: 3
Idle cycle flag: flags, Start end flag: shared

DSU configuration:
Compatibility mode: None, Scrambling: Disabled, Subrate: Disabled
FEAC loopback: Inactive, Response: Disabled, Count: 0

DS3 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Algorithm: 2^15 - 1, 0.151, Pseudorandom (9), Induced error rate: 10e-0

Packet Forwarding Engine configuration:
Destination slot: 0, PLP byte: 1 (0x00)

CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>usec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>42499200</td>
<td>95</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>2236800</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface t3-0/2/0.0 (Index 66) (SNMP ifIndex 54) (Generation 8)
Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 4470, Generation: 17, Route table: 0
Flags: Protocol-Down
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255,
Generation: 24
show interfaces detail (E3, Frame Relay)

user@host> show interfaces e3-1/2/0 detail

Physical interface: e3-1/2/0, Enabled, Physical link is Up
  Interface index: 153, SNMP ifIndex: 49, Generation: 36
  Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, Speed: E3,
  Loopback: None, FCS: 16, Framing: G751
  Device flags : Present Running
  Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags : Keepalives DTE
  Hold-times : Up 0 ms, Down 0 ms
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI statistics:
    Input : 0 (last seen: never)
    Output: 5 (last sent 00:00:07 ago)
  DTE statistics:
    Enquiries sent : 5
Full enquiries sent: 0
Enquiry responses received: 0
Full enquiry responses received: 0

DCE statistics:
Enquiries received: 0
Full enquiries received: 0
Enquiry responses sent: 0
Full enquiry responses sent: 0

Common statistics:
Unknown messages received: 0
Asynchronous updates received: 0
Out-of-sequence packets received: 0
Keepalive responses timedout: 1
CoS queues: 4 supported, 4 in use
Last flapped: 2005-12-05 08:46:14 PST (02:27:27 ago)
Statistics last cleared: Never

Traffic statistics:
Input bytes: 0 0 bps
Output bytes: 806 0 bps
Input packets: 0 0 pps
Output packets: 44 0 pps

Queue counters:
0 best-effort
1 expedited-fo
2 assured-forw
3 network-cont

Active alarms: None
Active defects: None

Logical interface e3-1/2/0.0 (Index 66) (SNMP ifIndex 57) (Generation 15)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID

Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Transit statistics:
Input bytes: 0 0 bps
Output bytes: 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

Protocol inet, MTU: 4470, Generation: 24, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast:
198.51.100.255,
Generation: 38
DLCI 100
Flags: Down, DCE-Unconfigured
Total down time: 00:00:16 sec, Last down: 00:00:16 ago
Traffic statistics:
Input bytes :  0
Output bytes :  0
Input packets:  0
Output packets:  0

DLCI statistics:
Active DLCI :0  Inactive DLCI :1

show interfaces extensive (E3, Frame Relay)

user@host> show interfaces e3-1/2/0 extensive

Physical interface: e3-1/2/0, Enabled, Physical link is Up
Interface index: 153, SNMP ifIndex: 49, Generation: 36
Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, Speed: E3,
Loopback: None, FCS: 16, Framing: G751
Device flags : Present Running
Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : Keepalives DTE
Hold-times : Up 0 ms, Down 0 ms
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI statistics:
  Input : 0 (last seen: never)
  Output: 6 (last sent 00:00:02 ago)
DTE statistics:
  Enquiries sent : 5
  Full enquiries sent : 1
  Enquiry responses received : 0
  Full enquiry responses received : 0
DCE statistics:
  Enquiries received : 0
  Full enquiries received : 0
  Enquiry responses sent : 0
  Full enquiry responses sent : 0
Common statistics:
  Unknown messages received : 0
  Asynchronous updates received : 0
  Out-of-sequence packets received : 0
  Keepalive responses timedout : 1
CoS queues : 4 supported, 4 in use
Last flapped : 2005-12-05 08:46:14 PST (02:27:30 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes :  0  0 bps
Output bytes :  821  56 bps
Input packets:  0  0 pps
Output packets:  45  0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 21118, Bucket drops: 0,
  Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0,
  L2 mismatch timeouts: 0, H5 link CRC errors: 0, SRAM errors: 0,
  Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
  Resource errors: 0
Queue counters:     Queued packets Transmitted packets Dropped packets
0 best-effort     0 0 0
Chapter 14: Interface Operational Commands

1 expedited-fo  0  0  0
2 assured-forward  0  0  0
3 network-cont  44  44  0

Active alarms: None
Active defects: None

E3 media: Seconds Count State
PLL Lock  0  0  OK
Reframing  187  1  OK
AIS  0  0  OK
LOF  187  1  OK
LOS  187  1  OK
IDLE  0  0  OK
YELLOW  0  0  OK
BPV  0  0
EXZ  0  0
LCV  188  12303167
LES  188
SEFS  187
UAS  195

DSU configuration:
Compatibility mode: None, Scrambling: Disabled

E3 BERT configuration:
BERT time period: 10 seconds, Elapsed: 0 seconds
Algorithm: 2^15 - 1, 0.151, Pseudorandom (9), Induced Error rate: 10e-0

Packet Forwarding Engine configuration:
Destination slot: 1, PLP byte: 1 (0x00)

CoS information:
CoS transmit queue
<table>
<thead>
<tr>
<th>% best-effort</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>95</td>
<td>32649600</td>
<td>95</td>
<td>0</td>
<td>low</td>
</tr>
<tr>
<td>3 network-control</td>
<td>1718400</td>
<td>5</td>
<td>0</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface e3-1/2/0.0 (Index 66) (SNMP ifIndex 57) (Generation 15)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID

Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

Protocol inet, MTU: 4470, Generation: 24, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 198.51.100.0/24, Local: 198.51.100.1, Broadcast: 198.51.100.255,
Generation: 38
DLCI 100
Flags: Down, DCE-Unconfigured
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total down time</td>
<td>00:00:19 sec</td>
</tr>
<tr>
<td>Last down</td>
<td>00:00:19 ago</td>
</tr>
<tr>
<td>Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td>Input bytes</td>
<td>0</td>
</tr>
<tr>
<td>Output bytes</td>
<td>0</td>
</tr>
<tr>
<td>Input packets</td>
<td>0</td>
</tr>
<tr>
<td>Output packets</td>
<td>0</td>
</tr>
<tr>
<td>DLCI statistics:</td>
<td></td>
</tr>
<tr>
<td>Active DLCI</td>
<td>0</td>
</tr>
<tr>
<td>Inactive DLCI</td>
<td>1</td>
</tr>
</tbody>
</table>
show interfaces demux0 (Demux Interfaces)

Syntax
show interfaces demux0.logical-interface-number
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <snmp-index snmp-index>
  <statistics>

Release Information
Command introduced in Junos OS Release 9.0.

Description
(MX Series and M Series routers only) Display status information about the specified demux interface.

Options
  none—Display standard information about the specified demux interface.
  brief | detail | extensive | terse—(Optional) Display the specified level of output.
  descriptions—(Optional) Display interface description strings.
  media—(Optional) Display media-specific information about network interfaces.
  snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.
  statistics—(Optional) Display static interface statistics.

Required Privilege
view

Related Documentation
  • Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration

List of Sample Output
  show interfaces demux0 (Demux) on page 1609
  show interfaces demux0 (PPPoE over Aggregated Ethernet) on page 1610
  show interfaces demux0 extensive (Targeted Distribution for Aggregated Ethernet Links) on page 1611
  show interfaces demux0 (ACI Interface Set Configured) on page 1611

Output Fields
  Table 51 on page 1603 lists the output fields for the show interfaces demux0 (Demux Interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 51: show interfaces demux0 (Demux Interfaces) Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are described in the “Enabled Field” section under “Common Output Fields Description” on page 1152.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Physical link</td>
<td>Status of the physical link (Up or Down).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Admin</td>
<td>Administrative state of the interface (Up or Down).</td>
<td>terse</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link</td>
<td>Status of the physical link (Up or Down).</td>
<td>terse</td>
</tr>
<tr>
<td>Targeting summary</td>
<td>Status of aggregated Ethernet links that are configured with targeted distribution (primary or backup)</td>
<td>extensive</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Bandwidth allocated to the aggregated Ethernet links that are configured with targeted distribution.</td>
<td>extensive</td>
</tr>
<tr>
<td>Proto</td>
<td>Protocol family configured on the interface.</td>
<td>terse</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface. <strong>Software-Pseudo</strong> indicates a standard software interface with no associated hardware device.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: <strong>Internal</strong> (1) or <strong>External</strong> (2).</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Link type</td>
<td>Data transmission type.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Table 51: show interfaces demux0 (Demux 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>Link flags</td>
<td>Information about the link. Possible values are described in the “Link Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Physical info</td>
<td>Information about the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup address of the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IPv6 transit statistics—Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> These fields include dropped traffic and exception traffic, as those fields are not separately defined.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 51: show interfaces demux0 (Demux 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><strong>Input errors</strong></td>
<td>Input errors on the interface whose definitions are as follows:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant packet threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Input Rate</strong></td>
<td>Input rate in bits per second (bps) and packets per second (pps).</td>
<td>none</td>
</tr>
<tr>
<td><strong>Output errors</strong></td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td><strong>Output Rate</strong></td>
<td>Output rate in bps and pps.</td>
<td>none</td>
</tr>
<tr>
<td><strong>Logical Interface</strong></td>
<td>Name of the logical interface.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>SNMP Interface index number for the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>brief detail extensive</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>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>brief extensive none</td>
</tr>
<tr>
<td>ACI VLAN: Dynamic Profile</td>
<td>Name of the dynamic profile that defines the agent circuit identifier (ACI) interface set. If configured, the ACI interface set enables the underlying demux interface to create dynamic VLAN subscriber interfaces based on ACI information.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Demux</td>
<td>Specific IP demultiplexing (demux) values:</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• Underlying interface—The underlying interface that the demux interface uses.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Index—Index number of the logical interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Family—Protocol family configured on the logical interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Source prefixes, total—Total number of source prefixes for the underlying interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Destination prefixes, total—Total number of destination prefixes for the underlying interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prefix—in prefix</td>
<td></td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the specified interface set.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes, Output bytes—Number of bytes received and transmitted on the interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets, Output packets—Number of packets received and transmitted on the interface set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IPv6 transit statistics—Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Number of transit bytes and packets received and transmitted on the local interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table S1: show interfaces demux0 (Demux 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>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The packet and byte counts in these fields include traffic that is dropped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and does not leave the router.</td>
<td></td>
</tr>
<tr>
<td>Input bytes</td>
<td>Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output bytes</td>
<td>Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input packets</td>
<td>Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

**IPv6 Transit statistics**

Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.

**NOTE:** The packet and byte counts in these fields include traffic that is dropped and does not leave the router.

- Input bytes—Number of bytes received on the interface.
- Output bytes—Number of bytes transmitted on the interface.
- Input packets—Number of packets received on the interface.
- Output packets—Number of packets transmitted on the interface.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packets</td>
<td>Number of packets received on the interface.</td>
<td>none</td>
</tr>
<tr>
<td>Output packets</td>
<td>Number of packets transmitted on the interface.</td>
<td>none</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family. Possible values are described in the “Protocol Field” section</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>under “Common Output Fields Description” on page 1152.</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Maximum labels</td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Route table in which the logical interface address is located. For example, 0</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>refers to the routing table inet.0.</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Mac-Validate Failures</td>
<td>Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags. Possible values are described in the “Addresses Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive statistics none</td>
</tr>
</tbody>
</table>
Table 51: show interfaces demux0 (Demux 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>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive terse</td>
</tr>
<tr>
<td>Remote</td>
<td>IP address of the remote interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Link</td>
<td>Name of the physical interfaces for member links in an aggregated Ethernet bundle for a PPPoE over aggregated Ethernet configuration. PPPoE traffic goes out on these interfaces.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Dynamic-profile</td>
<td>Name of the PPPoE dynamic profile assigned to the underlying interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Service Name Table</td>
<td>Name of the PPPoE service name table assigned to the PPPoE underlying interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Max Sessions</td>
<td>Maximum number of dynamic PPPoE logical interfaces that the router can activate on the underlying interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Duplicate Protection</td>
<td>State of duplicate protection: On or Off. Duplicate protection prevents the activation of another dynamic PPPoE logical interface on the same underlying interface when a dynamic PPPoE logical interface for a client with the same MAC address is already active on that interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Direct Connect</td>
<td>State of the configuration to ignore DSL Forum VSAs: On or Off. When configured, the router ignores any of these VSAs received from a directly connected CPE device on the interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>AC Name</td>
<td>Name of the access concentrator.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces demux0 (Demux)

```
user@host> show interfaces demux0
Physical interface: demux0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 79, Generation: 129
  Type: Software-Pseudo, Link-level type: Unspecified, MTU: 9192, Clocking: 1, Speed: Unspecified
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type : Full-Duplex
  Link flags : None
  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:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

IPv6 transit statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Input errors:
- Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
- Policed discards: 0, Resource errors: 0

Output errors:
- Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
- Resource errors: 0

Logical interface demux0.0 (Index 87) (SNMP ifIndex 84) (Generation 312)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Demux:
- Underlying interface: ge-2/0/1.0 (Index 74)

Family Inet Source prefixes, total 1
Prefix: 203.0.113/24
Traffic statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>1554</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>37</td>
</tr>
</tbody>
</table>

IPv6 transit statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Local statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>1554</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>37</td>
</tr>
</tbody>
</table>

Transit statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

IPv6 transit statistics:
<table>
<thead>
<tr>
<th>Type</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>packets</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Protocol inet, MTU: 1500, Generation: 395, Route table: 0
Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 203.0.113/24, Local: 203.0.113.13, Broadcast: 203.0.113.255,
  Generation: 434

show interfaces demux0 (PPPoE over Aggregated Ethernet)

user@host> show interfaces demux0.100
Logical interface demux0.100 (Index 76) (SNMP ifIndex 61160)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]
Encapsulation: ENET2
Demux:
   Underlying interface: ae0 (Index 199)
Link:
   ge-1/0/0
   ge-1/1/0
Input packets : 0
Output packets: 0
Protocol pppoe
   Dynamic Profile: pppoe-profile,
   Service Name Table: service-table1,
   Max Sessions: 100, Duplicate Protection: On,
   Direct Connect: Off,
   AC Name: pppoe-server-1

show interfaces demux0 extensive (Targeted Distribution for Aggregated Ethernet Links)
user@host> show interfaces demux0.1073741824 extensive

Logical interface demux0.1073741824 (Index 75) (SNMP ifIndex 558) (Generation 346)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.1 ]  Encapsulation: ENET2
Demux:
   Underlying interface: ae0 (Index 201)
Link:
   ge-1/0/0
   ge-1/1/0
   ge-2/0/7
   ge-2/0/8
Targeting summary:
   ge-1/1/0, primary, Physical link is Up
   ge-2/0/8, backup, Physical link is Up
Bandwidth: 1000mbps

show interfaces demux0 (ACI Interface Set Configured)
user@host> show interfaces demux0.1073741827

Logical interface demux0.1073741827 (Index 346) (SNMP ifIndex 527)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.1802 0x8100.302 ]  Encapsulation: ENET2
Demux: Source Family Inet
ACI VLAN:
   Dynamic Profile: aci-vlan-set-profile
   Demux:
   Underlying interface: ge-1/0/0 (Index 138)
   Input packets : 18
   Output packets: 16
   Protocol inet, MTU: 1500
   Flags: Sendcast-pkt-to-re, Unnumbered
   Donor interface: lo0.0 (Index 322)
   Preferred source address: 203.0.113.202
   Addresses, Flags: Primary Is-Default Is-Primary
      Local: 203.0.113.119
   Protocol pppoe
   Dynamic Profile: aci-vlan-pppoe-profile,
Service Name Table: None,
Max Sessions: 32000, Max Sessions VSA Ignore: Off,
Duplicate Protection: On, Short Cycle Protection: Off,
Direct Connect: Off,
AC Name: nbc
show interfaces extensive

**Syntax**

```
show interfaces extensive
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
- Command introduced in Junos OS Release 17.2 for PT1000 and PTX10008 Packet Transport Routers.

**Description**

Display extensive information about all interfaces configured on the router.
NOTE:

- At some times, the cumulative byte counters displayed with the show interfaces extensive command on the 10-Gigabit Ethernet MPC with SFP+ is not always increasing and cumulative and does not give the correct results. There is a time lag in collecting these statistics, during which the display might decrease or go from a nonzero number to zero. Eventually, the counter will display the correct result.

- When the show interfaces extensive command is executed on a router with an MPC or a T4000 Type 5 FPC, the Input packet rejects counter of the Filter statistics field also displays statistics related to the following packet errors:
  - Invalid VLAN range
  - Tagged packet received on an untagged interface

- When the show interfaces extensive command is executed on an interface that is configured on a T4000 Type 5 FPC, the IPv6 transit statistics field displays:
  - Total statistics (sum of transit and local statistics) at the physical interface level
  - Transit statistics at the logical interface level

- When the show interfaces extensive command is executed on an aggregate interface in a T1600 Core Router, the IPv6 Input bytes is displayed for an aggregate interface. However, the IPv6 Input bytes is always zero on a member link of an aggregated bundle even when there is IPv6 transit traffic on the member link. This is because the logical interface index of the aggregate logical interface is updated but not the logical interface of the member links in the channel lookup table.

- The Output packets field under the Traffic statistics section in the output of the show interfaces extensive command includes both IPv4 and IPv6 packets. For example, in a scenario in which both IPv4 and IPv6 packets are being mirrored on the same interface and when you deactivate an IPv4 port-mirroring instance on the chassis, the output of the show interfaces extensive command shows a value in the Output packets field of the Traffic statistics section, which is the value of IPv6 packets that are mirrored and not of the IPv4 packets. This behavior is expected.

- For IQ2 PIC interfaces, the output of the show interfaces extensive command displays byte statistics that includes Layer 2 headers.

- If there are active OTN defects when an ISSU is performed, and the defect persists after the upgrade completes, the OTN alarm count is incremented by 1. For example, if an OTN alarm is active with a count of 1 and the defect remains after ISSU, the alarm count is incremented to 2. This behavior is expected.
Options
This command has no options.

Required Privilege
Level
view

List of Sample Output
show interfaces extensive (Circuit Emulation) on page 1615
show interfaces extensive (Fast Ethernet) on page 1616
show interfaces extensive (Gigabit Ethernet) on page 1618
show interfaces extensive (10-Gigabit Ethernet) on page 1618
show interfaces extensive (IQ2 and IQ2E) on page 1621
show interfaces extensive (100-Gigabit Ethernet Type 4 PIC with CFP) on page 1624
show interfaces extensive (PTX5000 Packet Transport Router) on page 1626
show interfaces extensive (PTX10008 Routers) on page 1628
show interfaces extensive (PTX1000 Routers) on page 1633
show interfaces extensive (MX Series Routers) on page 1635
show interfaces extensive (MX480 Router with MPC5E and 10-Gigabit Ethernet OTN Interface) on page 1637
show interfaces extensive (MX480 Router with MPC5E and 100-Gigabit Ethernet OTN Interface) on page 1639
show interfaces extensive ((MX960 Router with MPC3E and 100-Gigabit DWDM OTN MIC) on page 1641
show interfaces extensive (PTX3000 Router with 5-port 100-Gigabit DWDM OTN PIC) on page 1644
show interfaces extensive ( on page 1647
show interfaces extensive (MX2020 Router with MPC6E and OTN MIC) on page 1647
show interfaces extensive (MX2010 Router with MPC6E and 100-Gigabit Ethernet OTN Interface) on page 1650
show interfaces extensive (MX2010 Router with MPC6E and 10-Gigabit Ethernet Interface) on page 1652
show interfaces extensive (T4000 Routers with Type 5 FPCs) on page 1653
show interfaces extensive (Aggregated Ethernet) on page 1655

Output Fields
For more information, see the output fields table for the particular interface type in which you are interested. For information about destination class and source class statistics, see the "Destination Class Field" section and the "Source Class Field" section under "Common Output Fields Description" on page 1152. For sample output for specific interfaces, see the other topics in this collection.

Sample Output
show interfaces extensive (Circuit Emulation)

If a Circuit Emulation (CE) PIC is configured for SAToP pseudowire, then pseudowire statistics are displayed in the CE information section of the show interface extensive output. If SAToP pseudowire is not configured on the CE PIC, then all CE information counters display 0 (zero).

user@host> show interface t1-0/0/0 extensive
Physical interface: t1-0/0/0, Enabled, Physical Link: Up
Interface index: 61441
Speed: 1.54 Mbps, Loopback: Disabled
Operational state: Enabled, Encapsulation: Trans
Encoding: b8zs, Framing: unframe, Build-out: 0-30
Inversion: enable, Clock source: master
Description:
Traffic statistics:
T1 media: Seconds
ES 1643
SES 1643
CE Info Packets Bytes
CE Rx 2395529 306627712
CE Tx 2396259 306721152
CE Rx Drop 0 0
CE Tx Drop 0 0
CE Overrun Events: 0
CE Underrun Events: 0

Sample Output

show interfaces extensive (Fast Ethernet)

user@host> show interfaces fe-0/2/1 extensive

Physical interface: fe-0/2/0, Enabled, Physical link is Up
Interface index: 129, SNMP ifIndex: 23, Generation: 130
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags: Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues: 4 supported, 4 maximum usable queues
Hold-times: Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped: 2006-04-16 23:00:41 PDT (02:08:05 ago)
Statistics last cleared: 2006-04-16 21:42:00 PDT (03:26:46 ago)
Traffic statistics:
Input bytes: 17539 152 bps
Output bytes: 92968 224 bps
Input packets: 348 0 pps
Output packets: 1349 0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 4 supported, 4 in use
Queue counters:
0 best-effort Queued packets Transmitted packets Dropped packets
0 66 66 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
### Interface Operational Commands

#### MAC Statistics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>24721</td>
<td>105982</td>
</tr>
<tr>
<td>Total packets</td>
<td>348</td>
<td>1349</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>347</td>
<td>430</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>1</td>
<td>37</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>882</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Filter Statistics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet count</td>
<td>348</td>
</tr>
<tr>
<td>Input packet rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input SA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Output packet count</td>
<td>1349</td>
</tr>
<tr>
<td>Output packet pad count</td>
<td>0</td>
</tr>
<tr>
<td>Output packet error count</td>
<td>0</td>
</tr>
</tbody>
</table>

CAM destination filters: 3, CAM source filters: 0

#### Autonegotiation Information

- **Negotiation status:** Complete
- **Link partner:**
  - **Link mode:** Full-duplex, Flow control: None, Remote fault: OK

#### Packet Forwarding Engine Configuration

- **Destination slot:** 0

#### CoS Information

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth %</th>
<th>Buffer %</th>
<th>Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>95000000</td>
<td>low</td>
<td>none</td>
</tr>
<tr>
<td>3 network-control</td>
<td>55</td>
<td>50000000</td>
<td>low</td>
<td>none</td>
</tr>
</tbody>
</table>

#### Logical Interface Status

- **Index:** 66, **SNMP ifIndex:** 46, **Generation:** 133
- **Flags:** SNMP-Traps Encapsulation: ENET2
- **Protocol:** inet, **MTU:** 1500, **Generation:** 142, **Route table:** 0
- **Flags:** DCU, SCU-out

#### Destination Class Traffic

<table>
<thead>
<tr>
<th>Destination class</th>
<th>Packets (packet-per-second)</th>
<th>Bytes (bits-per-second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>silv1_new</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silv2_new</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silv_misc</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>silver4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Packets (packet-per-second)</td>
<td>Bytes (bits-per-second)</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>gold1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gold2</td>
<td>16600</td>
<td>1062400</td>
</tr>
<tr>
<td>gold3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Addresses, Flags: Is-Preferred Is-Primary

show interfaces extensive (Gigabit Ethernet)

user@host> show interfaces ge-5/0/0.0 extensive

Logical interface ge-5/0/0.0 (Index 71) (SNMP ifIndex 1930) (Generation 139)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Traffic statistics:
Input bytes : 0
Output bytes : 42
Input packets: 0
Output packets: 1
Local statistics:
Input bytes : 0
Output bytes : 42
Input packets: 0
Output packets: 1
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Output Filters: f-any
Protocol inet, MTU: 1500, Generation: 155, Route table: 0
Output Filters: f-inet,
Addresses, Flags: Is-Preferred Is-Primary
  Generation: 170
Protocol multiservice, MTU: Unlimited, Generation: 156, Route table: 0
Flags: Is-Primary
Policer: Input: __default_arp_policer__

show interfaces extensive (10-Gigabit Ethernet)

user@host> show interfaces xe-2/1/0 extensive

Physical interface: xe-2/1/0, Enabled, Physical link is Up
Interface index: 258, SNMP ifIndex: 762, Generation: 2046
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error: None, Loopback: None, Source filtering: Disabled,
Flow control: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped   : 2011-12-17 00:19:02 PST (07:36:37 ago)
Statistics last cleared: 2011-12-17 07:55:24 PST (00:00:15 ago)
Traffic statistics:
<table>
<thead>
<tr>
<th></th>
<th>Input bytes</th>
<th>Output bytes</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>110000</td>
<td>0</td>
<td>1000</td>
<td>0</td>
</tr>
</tbody>
</table>
| IPv6 transit statistics:
|                  | Input bytes | Output bytes | Input packets | Output packets |
|                  | 110000      | 0            | 1000          | 0             |
| Input errors:
|                  | Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0 |
| Output errors:
|                  | Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0 |
| Egress queues:   | 8 supported, 4 in use |
| Queue counters:  | Queued packets | Transmitted packets | Dropped packets |
| 0 best-effort    | 0            | 0             | 0             |
| 1 expedited-fo   | 0            | 0             | 0             |
| 2 assured-forw   | 0            | 0             | 0             |
| 3 network-cont   | 0            | 0             | 0             |
| Queue number:    | Mapped forwarding classes |
| 0                | best-effort  |
| 1                | expedited-forwarding |
| 2                | assured-forwarding |
| 3                | network-control |
| Active alarms    | None         |
| Active defects   | None         |
| PCS statistics   | Seconds      |
| Bit errors       | 0            |
| Errored blocks   |              |
| MAC statistics   | Receive | Transmit |
| Total octets     | 128000 | 0        |
| Total packets    | 1000   | 0        |
| Unicast packets  | 1000   | 0        |
| Broadcast packets| 0      | 0        |
| Multicast packets| 0      | 0        |
| CRC/Align errors | 0      | 0        |
| FIFO errors      | 0      | 0        |
| MAC control frames| 0    | 0        |
### Interface Statistics

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC pause frames</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
</tr>
</tbody>
</table>

**Filter statistics:**
- Input packet count: 1000
- Input packet rejects: 0
- Input DA rejects: 0
- Input SA rejects: 0
- Output packet count: 0
- Output packet pad count: 0
- Output packet error count: 0

**CAM destination filters:** 0, **CAM source filters:** 0

**Packet Forwarding Engine configuration:**
- Destination slot: 2

**CoS information:**
- Direction: Output
- CoS transmit queue limits:
  - 0 best-effort: 95% bandwidth, 95% buffer priority
  - 3 network-control: 5% bandwidth, 5% buffer priority

**Packet transmit statistics:**
- Disabled

#### Logical Interface xe-2/1/0.0 (Index 83) (SNMP ifIndex 1677) (Generation 10082)

**Flags:** SNMP-Traps 0x40040000
**Encapsulation:** ENET2

**Traffic statistics:**
- Input bytes: 110000
- Output bytes: 0
- Input packets: 1000
- Output packets: 0

**IPv6 transit statistics:**
- Input bytes: 55000
- Output bytes: 0
- Input packets: 500
- Output packets: 0

**Local statistics:**
- Input bytes: 55000
- Output bytes: 0
- Input packets: 500
- Output packets: 0

**Transit statistics:**
- Input bytes: 55000, 0 bps
- Output bytes: 0, 0 bps
- Input packets: 500, 0 pps
- Output packets: 0, 0 pps

**IPv6 transit statistics:**
- Input bytes: 55000
- Output bytes: 0
- Input packets: 500
- Output packets: 0

**Protocol inet6, MTU: 1500, Generation: 23739, Route table: 0**
- Addresses, Flags: Is-Preferred Is-Primary
- Destination: 2001:0db8:0a0b:12f0:0000:0000:0000:112, Local: 2001:0db8:0a0b:12f0:0000:0000:0000:0001
**show interfaces extensive (IQ2 and IQ2E)**

```plaintext
user@host> show interfaces ge-3/2/2 extensive

Physical interface: ge-3/2/2, Enabled, Physical link is Up
Interface index: 156, SNMP ifIndex: 548, Generation: 159
Link-level type: Ethernet, MTU: 1518, Speed: 1000mbps, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues : 8 supported, 8 maximum usable queues
Schedulers : 128
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped : 2010-03-17 04:03:11 PDT (00:45:30 ago)
Statistics last cleared: Never
Traffic statistics:
<table>
<thead>
<tr>
<th></th>
<th>Input bytes</th>
<th>Output bytes</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1716096</td>
<td>1716448</td>
<td>13407</td>
<td>13411</td>
</tr>
</tbody>
</table>
IPv6 total statistics:
<table>
<thead>
<tr>
<th></th>
<th>Input bytes</th>
<th>Output bytes</th>
<th>Input packets</th>
<th>Output packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1716096</td>
<td>1716096</td>
<td>13407</td>
<td>13407</td>
</tr>
</tbody>
</table>
Ingress traffic statistics at Packet Forwarding Engine:
<table>
<thead>
<tr>
<th></th>
<th>Input bytes</th>
<th>Input packets</th>
<th>Drop bytes</th>
<th>Drop packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1716096</td>
<td>13407</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 1, L2 mismatch timeouts: 0, FIFO errors: 0,
Resource errors: 0
Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Ingress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 13407 13407
0 1 expedited-fo 0 0
0 2 assured-forw 0 0
0 3 network-cont 0 0
0 Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
```
packets

<table>
<thead>
<tr>
<th>Type</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>13407</td>
<td>13407</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Active alarms : None
Active defects : None

MAC statistics: Receive Transmit
- Total octets: 1716096 1716448
- Total packets: 13407 13411
- Unicast packets: 13407 13407

Filter statistics:
- Input packet count: 13407
- Output packet count: 13411

Autonegotiation information:
- Negotiation status: Complete
- Link partner:
  - Link mode: Full-duplex, Flow control: None, Remote fault: OK
- Local resolution:
  - Flow control: Symmetric, Remote fault: Link OK

Packet Forwarding Engine configuration:
- Destination slot: 3

CoS information:
- Direction: Output

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95%</td>
<td>950000000 bps</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5%</td>
<td>500000000 bps</td>
</tr>
</tbody>
</table>

Direction: Input

CoS information:

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95%</td>
<td>950000000 bps</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5%</td>
<td>500000000 bps</td>
</tr>
</tbody>
</table>
Logical interface ge-3/2/2.0 (Index 83) (SNMP ifIndex 6080) (Generation 148)

Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ] Encapsulation: ENET2

Traffic statistics:
- Input bytes: 0
- Output bytes: 336
- Input packets: 0
- Output packets: 4

IPv6 total statistics:
- Input bytes: 1716096
- Output bytes: 1716096
- Input packets: 13407
- Output packets: 13407

Local statistics:
- Input bytes: 0
- Output bytes: 336
- Input packets: 0
- Output packets: 4

Transit statistics:
- Input bytes: 0, 0 bps
- Output bytes: 0, 0 bps
- Input packets: 0, 0 pps
- Output packets: 0, 0 pps

IPv6 total statistics:
- Input bytes: 1716096
- Output bytes: 1716096
- Input packets: 13407
- Output packets: 13407

Protocol inet6, MTU: 1500, Generation: 159, Route table: 0
- Flags: Is-Primary
- Addresses, Flags: Is-Default Is-Primary
- Destination: Unspecified, Local: 2000::2
- Generation: 146
- Addresses, Flags: Is-Preferred
- Destination: fe80::/64, Local: fe80::214:f600:6412:86fa

Protocol multiservice, MTU: Unlimited, Generation: 148
- Generation: 160, Route table: 0
- Policer: Input: __default_arp_policer__

Logical interface ge-3/2/2.32767 (Index 84) (SNMP ifIndex 6081) (Generation 149)

Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2

Traffic statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

Local statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

Transit statistics:
- Input bytes: 0, 0 bps
- Output bytes: 0, 0 bps
- Input packets: 0, 0 pps
- Output packets: 0, 0 pps

Protocol multiservice, MTU: Unlimited, Generation: 161, Route table: 0
show interfaces extensive (100-Gigabit Ethernet Type 4 PIC with CFP)

```
user@host> show interfaces et-0/0/0:0 extensive

Physical interface: et-0/0/0:0, Enabled, Physical link is Down
  Interface index: 156, SNMP ifIndex: 516, Generation: 163
  Link-level type: Ethernet, MTU: 9192, Speed: 50000mbps, BPDU Error: None,
  MAC-REWRITE Error: None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Damping : half-life: 5 sec, max-suppress: 20 sec, reuse 1000, suppress: 2000, state: enabled
  Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
  Last flapped : 2010-01-07 16:36:49 PST (18:02:35 ago)
  Statistics last cleared: Never

Traffic statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps

IPv6 transit statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0

Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0

Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 8 in use

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 DEFAULT, NC-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 REALTIME</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 PRIVATE, NC-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 CONTROL</td>
<td>1253</td>
<td>1253</td>
<td>0</td>
</tr>
<tr>
<td>4 BC-H, CLASS_</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 BC-M, CLASS_</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6 IA, CLASS_V_</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7 CLASS_S_OUTP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Queue       Mapped Forwarding Class
0        DEFAULT, NC-Q0
1        REALTIME
2        PRIVATE, NC-Q1
3        CONTROL
4        BC-H, CLASS-Q4
5        BC-M, CLASS-Q5
6        IA, CLASS_V_OUTPUT
7        CLASS_S_OUTPUT
Active alarms : None
Active defects : None
MAC statistics:                                          Receive        Transmit
Total octets                              0                0
Total packets                             0                0
Unicast packets                          0                0
Broadcast packets                        0                0
Multicast packets                        0                0
CRC/Align errors                         0                0
FIFO errors                              0                0
MAC control frames                       0                0
MAC pause frames                         0                0
Oversized frames                         0                0
Jabber frames                            0                0
Fragment frames                          0                0
VLAN tagged frames                       0                0
Code violations                          0                0
Packet Forwarding Engine configuration:
   Destination slot: 0
   CoS information:
   Direction : Output
   CoS transmit queue               Bandwidth               Buffer Priority Limit
   %            bps     %           usec
   0 best-effort            95    47500000000    95              0      low none
   3 network-control         5     2500000000     5              0      low none
Logical interface et-0/0/0:0.0 (Index 68) (SNMP ifIndex 546) (Generation 161)
   Flags: Deviet-Down SNMP-Traps Encapsulation: ENET2
Traffic statistics:
   Input bytes :                    0
   Output bytes :                    0
   Input packets:                    0
   Output packets:                    0
Local statistics:
   Input bytes :                    0
   Output bytes :                    0
   Input packets:                    0
   Output packets:                    0
Transit statistics:
   Input bytes :                    0                        0 bps
   Output bytes :                    0                        0 bps
   Input packets:                    0                        0 pps
   Output packets:                    0                        0 pps
Protocol inet, MTU: 9178, Generation: 220, Route table: 0
   Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Protocol mpls, MTU: 9166, Maximum labels: 3, Generation: 221, Route table: 0
show interfaces extensive (PTX5000 Packet Transport Router)

user@host> show interfaces et-0/0/6 extensive

Physical interface: et-0/0/6, Enabled, Physical link is Up
  Interface index: 347, SNMP ifIndex: 531, Generation: 350
  Link-level type: Ethernet, MTU: 1514, Speed: 40Gbps, BPDU Error: None, Loop
  Detect PDU Error: None, Loopback: Disabled, Source filtering: Disabled, Flow
  control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Damping : half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsuppressed
  Current address: 30:b6:4f:02:29:06, Hardware address: 30:b6:4f:02:29:06
  Statistics last cleared: 2017-02-16 20:33:02 PST (00:02:17 ago)
  Traffic statistics:
    Input bytes : 1760000 0 bps
    Output bytes : 1540000 0 bps
    Input packets: 16000 0 pps
    Output packets: 14000 0 pps
  IPv6 transit statistics:
    Input bytes : 880000
    Output bytes : 770000
    Input packets: 8000
    Output packets: 7000
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3
    incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0,
    Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
    FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:
    Queued packets Transmitted packets Dropped packets
    0 7000 7000 0
    1 0 0 0
    2 0 0 0
    3 7000 7000 0
  Queue number: Mapped forwarding classes
    0 best-effort
    1 expedited-forwarding
    2 assured-forwarding
    3 network-control
  Active alarms : None
  Active defects : None
  PCS statistics
    Bit errors 0
Errored blocks 0

MAC statistics:                      Receive         Transmit
Total octets                       2048000          1792000
Total packets                        16000            14000
Unicast packets                      16000            14000
Broadcast packets                        0                0
Multicast packets                        0                0
CRC/Align errors                         0                0
FIFO errors                              0                0
MAC control frames                       0                0
MAC pause frames                         0                0
Oversized frames                        0                0
Jabber frames                           0                0
Fragment frames                          0                0
VLAN tagged frames                       0                0
Code violations                          0                0

Filter statistics:
Input packet count                     0                0
Input packet rejects                   0                0
Input DA rejects                       0                0
Input SA rejects                       0                0
Output packet count                     0                0
Output packet pad count                 0                0
Output packet error count               0                0

CAM destination filters: 0, CAM source filters: 0

Packet Forwarding Engine configuration:
    Destination slot: 0 (0x00)
CoS information:
    Direction : Output
    CoS transmit queue
     CoS          Limit       Bandwidth      Buffer Priority
                    %          bps  %        usec
0 best-effort    0           0       0      low
3 network-control 0           0       0      low

Preclassifier statistics:
    Traffic Class  Received Packets  Transmitted Packets  Dropped
    best-effort    0                      0
    best-effort    0                      0
    best-effort    0                      0
    best-effort    0                      0
    best-effort    0                      0
    best-effort    0                      0
    best-effort    0                      0

Link Degrade :  
    Link Monitoring : Disable
    Interface transmit statistics: Disabled

Logical interface et-0/0/6.0 (Index 93) (SNMP ifIndex 841) (Generation 158)
show interfaces extensive (PTX10008 Routers)

user@host> show interfaces ae0 extensive

Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 917, SNMP ifIndex: 817, Generation: 4436
  Link-level type: Ethernet, MTU: 1518, Speed: 20Gbps, BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
  Minimum bandwidth needed: 1bps
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000

Flags: Up SNMP-Traps 0x4004000 Encapsulation: ENET2
Traffic statistics:
  Input bytes : 1760000
  Output bytes : 1540000
  Input packets: 16000
  Output packets: 14000
  IPv6 transit statistics:
    Input bytes : 880000
    Output bytes : 770000
    Input packets: 8000
    Output packets: 7000
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 1760000 0 bps
  Output bytes : 1540000 0 bps
  Input packets: 16000 0 pps
  Output packets: 14000 0 pps
  IPv6 transit statistics:
    Input bytes : 880000
    Output bytes : 770000
    Input packets: 8000
    Output packets: 7000
Protocol inet, MTU: 1500
  Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new
  hold cnt: 0, NH drop cnt: 0
  Generation: 206, Route table: 0
  Flags: Sendbcast-pkt-to-re
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 11.0.0/24, Local: 11.0.0.2, Broadcast: 11.0.0.255, Generation:
    228
Protocol inet6, MTU: 1500
  Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new
  hold cnt: 0, NH drop cnt: 0
  Generation: 207, Route table: 0
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 1100::/120, Local: 1100::2
  Generation: 230
  Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::32b6:4fff:fe02:2906
Protocol multiservice, MTU: Unlimited, Generation: 232
  Generation: 208, Route table: 0
  Policer: Input: __default_arp_policer__
Current address: 30:b6:4f:e9:7c:05, Hardware address: 30:b6:4f:e9:7c:05
Last flapped   : 2017-04-10 05:20:29 PDT (00:03:52 ago)
Statistics last cleared: 2017-04-10 05:21:52 PDT (00:02:29 ago)
Traffic statistics:
Input bytes   : 36463816334                    0 bps
Output bytes  : 36463816334                    0 bps
Input packets : 24671053                     0 pps
Output packets: 24671053                     0 pps
IPv6 transit statistics:
Input bytes   : 18231905950
Output bytes  : 18231905950
Input packets : 12335525
Output packets: 12335525
MAC statistics: Receive                     Transmit
Broadcast packets                       0                0
Multicast packets                        0                0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0    24671053    24671053                0
1     0          0                     0
2     0          0                     0
3     0          0                     0
Queue number: Mapped forwarding classes
0  best-effort
1  expedited-forwarding
2  assured-forwarding
3  network-control
Logical interface ae0.0 (Index 99) (SNMP ifIndex 832) (Generation 43813)
Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.2 ] Encapsulation: ENET2
Statistics Packets pps Bytes bps
Bundle:
Input : 4934211 0 7292763858 0
Output: 4934211 0 7292763858 0
Adaptive Statistics:
Adaptive Adjusts: 0
Adaptive Scans : 0
Adaptive Updates: 0
Link:
et-0/0/28:0.0
Input : 4934211 0 7292763858 0
Output: 4934211 0 7292763858 0
et-0/0/28:3.0
Input : 0 0 0 0
Output: 0 0 0 0
Aggregate member links: 2
Interfaces Fundamentals for Routing Devices

Marker Statistics:  Marker Rx  Resp Tx  Unknown Rx  Illegal Rx
et-0/0/28:0.0     0        0        0        0
et-0/0/28:3.0     0        0        0        0

Protocol inet, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new
hold cnt: 0, NH drop cnt: 0
Generation: 89219, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 21.0.0.0/30, Local: 21.0.0.1, Broadcast: 21.0.0.3, Generation:
62420

Protocol inet6, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 2, Curr new
hold cnt: 0, NH drop cnt: 0
Generation: 89220, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 3001::1500:0/126, Local: 3001::1500:1
Generation: 62422
    Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::32b6:4f00:2e9:7c05
Protocol multiservice, MTU: Unlimited, Generation: 62424
Generation: 89221, Route table: 0
    Policer: Input: __default_arp_policer__

Logical interface ae0.1 (Index 100) (SNMP ifIndex 833) (Generation 43814)
Flags: Up SNMP-Traps Ox4000 VLAN-Tag [ Ox8100.3 ] Encapsulation: ENET2

Statistics       Packets      pps      Bytes      bps
Bundle:
    Input:  4934211  0    7292763858  0
    Output:  4934211  0    7292763858  0

Adaptive Statistics:
    Adaptive Adjusts:  0
    Adaptive Scans :  0
    Adaptive Updates:  0

Link:
et-0/0/28:0.1
    Input:  0    0    0    0
    Output:  0    0    0    0
et-0/0/28:3.1
    Input:  4934211  0    7292763858  0
    Output:  0    0    0    0

Marker Statistics:  Marker Rx  Resp Tx  Unknown Rx  Illegal Rx
et-0/0/28:0.1     0        0        0        0
et-0/0/28:3.1     0        0        0        0

Protocol inet, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new
hold cnt: 0, NH drop cnt: 0
Generation: 89222, Route table: 0
    Flags: Sendcast-pkt-to-re
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 21.0.0.0/30, Local: 21.0.0.5, Broadcast: 21.0.0.7, Generation:
62426

Protocol inet6, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 2, Curr new
hold cnt: 0, NH drop cnt: 0
Generation: 89223, Route table: 0
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 3001::1500:0/126, Local: 3001::1500:5
Generation: 62428
    Addresses, Flags: Is-Preferred
Logical interface ae0.2 (Index 101) (SNMP ifIndex 834) (Generation 43815)

Flags: Up SNMP-Traps [0x8100.4] Encapsulation: ENET2

Statistics

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>4934211</td>
<td>0</td>
<td>7292763858</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>4934211</td>
<td>0</td>
<td>7292763858</td>
<td>0</td>
</tr>
</tbody>
</table>

Adaptive Statistics:

- Adaptive Adjusts: 0
- Adaptive Scans: 0
- Adaptive Updates: 0

Link:

et-0/0/28:0.2

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>2467106</td>
<td>0</td>
<td>3646382668</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>4934211</td>
<td>0</td>
<td>7292763858</td>
<td>0</td>
</tr>
</tbody>
</table>

et-0/0/28:3.2

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>2467105</td>
<td>0</td>
<td>3646381190</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Marker Statistics:

et-0/0/28:0.2

- Marker Rx: 0
- Resp Tx: 0
- Unknown Rx: 0
- Illegal Rx: 0

et-0/0/28:3.2

- Marker Rx: 0
- Resp Tx: 0
- Unknown Rx: 0
- Illegal Rx: 0

Protocol inet, MTU: 1500

Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new hold cnt: 0, NH drop cnt: 0

Generation: 89225, Route table: 0

Flags: Sendicast-pkt-to-re

Addresses, Flags: Is-Preferred Is-Primary

Destination: 21.0.0.8/30, Local: 21.0.0.9, Broadcast: 21.0.0.11,

Generation: 62432

Protocol inet6, MTU: 1500

Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new hold cnt: 0, NH drop cnt: 0

Generation: 89226, Route table: 0

Addresses, Flags: Is-Preferred Is-Primary

Destination: 2001::1500:8/126, Local: 2001::1500:9

Generation: 62434

Addresses, Flags: Is-Preferred

Destination: fe80::/64, Local: fe80::32b6:4f00:4e9:7c05

Protocol multiservice, MTU: Unlimited, Generation: 62436

Generation: 89227, Route table: 0

Policer: Input: __default_arp_policer__

Logical interface ae0.3 (Index 102) (SNMP ifIndex 835) (Generation 43816)

Flags: Up SNMP-Traps [0x8100.5] Encapsulation: ENET2

Statistics

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>4934210</td>
<td>0</td>
<td>7292762380</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>4934210</td>
<td>0</td>
<td>7292762380</td>
<td>0</td>
</tr>
</tbody>
</table>

Adaptive Statistics:

- Adaptive Adjusts: 0
- Adaptive Scans: 0
- Adaptive Updates: 0

Link:

et-0/0/28:0.3

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>4934210</td>
<td>0</td>
<td>7292762380</td>
<td>0</td>
</tr>
<tr>
<td>Output</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Interface</td>
<td>Input</td>
<td>Output</td>
<td>Marker Rx</td>
<td>Resp Tx</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>--------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>et-0/0/28:3.3</td>
<td>4934210</td>
<td>7292762380</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et-0/0/28:0.3</td>
<td>4934210</td>
<td>7292762380</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>et-0/0/28:3.3</td>
<td>4934210</td>
<td>7292762380</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Protocol inet, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new hold cnt: 0, NH drop cnt: 0
Generation: 89228, Route table: 0
Flags: Sendcast-pkt-to-re
Addresses, Flags: Is-Preferred Is-Primary
Destination: 21.0.0.12/30, Local: 21.0.0.13, Broadcast: 21.0.0.15,
Generation: 62438
Protocol inet6, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 2, Curr new hold cnt: 0, NH drop cnt: 0
Generation: 89229, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 3001::1500::/126, Local: 3001::1500::d
Generation: 62440
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::32b6:4f00:5e9:7c05
Protocol multiservice, MTU: Unlimited, Generation: 62442
Generation: 89230, Route table: 0
Policer: Input: __default_arp_policer__

Logical interface ae0.4 (Index 103) (SNMP ifIndex 836) (Generation 43817)
Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.6 ] Encapsulation: ENET2
Statistics
<table>
<thead>
<tr>
<th>Bundle:</th>
<th>Packets</th>
<th>pps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input:</td>
<td>4934210</td>
<td>0</td>
<td>7292762380</td>
<td>0</td>
</tr>
<tr>
<td>Output:</td>
<td>4934210</td>
<td>0</td>
<td>7292762380</td>
<td>0</td>
</tr>
</tbody>
</table>

Adaptive Statistics:
Adaptive Adjusts: 0
Adaptive Scans: 0
Adaptive Updates: 0

Link:
et-0/0/28:0.4
Input: 2467105 0 3646381190 0
Output: 2467105 0 3646381190 0
et-0/0/28:3.4
Input: 2467105 0 3646381190 0
Output: 2467105 0 3646381190 0

Marker Statistics:
Marker Rx Resp Tx Unknown Rx Illegal Rx
et-0/0/28:0.4 0 0 0 0
et-0/0/28:3.4 0 0 0 0

Protocol inet, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 1, Curr new hold cnt: 0, NH drop cnt: 0
Generation: 89231, Route table: 0
Flags: Sendcast-pkt-to-re
Addresses, Flags: Is-Preferred Is-Primary
Destination: 21.0.0.16/30, Local: 21.0.0.17, Broadcast: 21.0.0.19,
Generation: 62444
Protocol inet6, MTU: 1500
Max nh cache: 100000, New hold nh limit: 100000, Curr nh cnt: 2, Curr new hold cnt: 0, NH drop cnt: 0
Generation: 89232, Route table: 0
Addresses, Flags: Is-Preferred Is-Primary
show interfaces extensive (PTX1000 Routers)

user@host> show interfaces et-0/0/48:1 extensive

Physical interface: et-0/0/48:1, Enabled, Physical link is Up
  Interface index: 306, SNMP ifIndex: 697, Generation: 311
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error: None, Loop Detect PDU Error: None, MAC-REWRITE Error: None, Loopback: None, Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Damping : half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsupported
  Last flapped : 2017-05-08 11:07:59 PDT (12:08:13 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  IPv6 transit statistics:
    Input bytes : 0
<table>
<thead>
<tr>
<th>Queue number:</th>
<th>Mapped forwarding classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
</tr>
<tr>
<td>1</td>
<td>expedited-forwarding</td>
</tr>
<tr>
<td>2</td>
<td>assured-forwarding</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
</tr>
</tbody>
</table>

Active alarms: None
Active defects: None

<table>
<thead>
<tr>
<th>PCS statistics</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>3</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC statistics:</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:
- Input packet count: 0
- Input packet rejects: 0
- Input DA rejects: 0
- Input SA rejects: 0
- Output packet count: 0
- Output packet pad count: 0
- Output packet error count: 0

CAM destination filters: 0, CAM source filters: 0

Packet Forwarding Engine configuration:
- Destination slot: 0 (0x00)

CoS information:
- Direction: Output
- CoS transmit queue

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### show interfaces extensive (MX Series Routers)

```
user@host> show interfaces xe-0/0/0 extensive

Physical interface: xe-0/0/0, Enabled, Physical link is Up
Interface index: 145, SNMP ifIndex: 592, Generation: 148
Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error: None,
Loopback: None, Source filtering: Disabled, Flow control: Enabled
Pad to minimum frame size: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped   : 2013-10-26 03:20:40 test (2w3d 03:15 ago)
Statistics last cleared: Never
Traffic statistics:
  Input  bytes  :                    0                    0 bps
  Output bytes :                    0                    0 bps
  Input  packets:                    0                    0 pps
  Output packets:                    0                    0 pps
IPv6 transit statistics:
  Input  bytes  :                   0
  Output bytes  :                   0
  Input  packets:                   0
  Output packets:                   0
Dropped traffic statistics due to STP State:
  Input  bytes  :                    0
  Output bytes  :                    0
  Input  packets:                    0
  Output packets:                    0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0,
  Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
  FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0                                0                    0                    0
  1                                0                    0                    0
  2                                0                    0                    0
```

---

```
### Limit

<table>
<thead>
<tr>
<th>Limit</th>
<th>%</th>
<th>bps</th>
<th>%</th>
<th>usec</th>
<th>low</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>9500000000</td>
<td>95</td>
<td>0</td>
<td>low</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>500000000</td>
<td>5</td>
<td>0</td>
<td>low</td>
</tr>
</tbody>
</table>

Link Degrade:
- Link Monitoring: Disable
- Interface transmit statistics: Disabled
```

---

Chapter 14: Interface Operational Commands
<table>
<thead>
<tr>
<th>Queue number:</th>
<th>Mapped forwarding classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
</tr>
<tr>
<td>1</td>
<td>expedited-forwarding</td>
</tr>
<tr>
<td>2</td>
<td>assured-forwarding</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
</tr>
</tbody>
</table>

Active alarms: LINK
Active defects: LINK

<table>
<thead>
<tr>
<th>PCS statistics</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>109</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>109</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC statistics:</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Queue number:</th>
<th>Mapped forwarding classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
</tr>
<tr>
<td>1</td>
<td>expedited-forwarding</td>
</tr>
<tr>
<td>2</td>
<td>assured-forwarding</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
</tr>
</tbody>
</table>

Active alarms: LINK
Active defects: LINK

<table>
<thead>
<tr>
<th>PCS statistics</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>109</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>109</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC statistics:</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total errors</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:
- Input packet count: 0
- Input packet rejects: 0
- Input DA rejects: 0
- Input SA rejects: 0
- Output packet count: 0
- Output packet pad count: 0
- Output packet error count: 0

CAM destination filters: 0, CAM source filters: 0

Packet Forwarding Engine configuration:
- Destination slot: 0

CoS information:
- Direction: Output
  - CoS transmit queue Bandwidth Buffer Priority
When an ASIC is wedged, the interfaces are brought down along with the IFD. The reason for the link down is displayed as **ASIC-Error** in the Device flags.

```
user@host> show interfaces xe-1/0/0 extensive
```

Physical interface: xe-1/0/0, Administratively down, Physical link is Down
- Interface index: 147, SNMP ifIndex: 563, Generation: 150
- Link-level type: Ethernet, MTU: 1514, MRU: 0, LAN-PHY mode, Speed: 10Gbps, BPDU Error: None, Loop Detect PDU Error: None,
- MAC-REWRITE Error: None, Loopback: None, Source filtering: Disabled, Flow control: Disabled
- Pad to minimum frame size: Disabled
- Device flags: Present Running Down ASIC-Error
- Interface flags: Hardware-Down Down Internal: 0x4000
- Link flags: None
- CoS queues: 8 supported, 8 maximum usable queues
- Schedulers: 0
- Hold-times: Up 0 ms, Down 0 ms
- Damping: half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsuppressed
- Current address: cc:e1:7f:a8:05:4a, Hardware address: cc:e1:7f:a8:05:4a
- Last flapped: 2017-06-05 17:20:54 PDT (00:03:51 ago)
- Statistics last cleared: Never

```
show interfaces extensive (MX480 Router with MPC5E and 10-Gigabit Ethernet OTN Interface)
```

```
user@host> show interfaces xe-0/0/3 extensive
```

Physical interface: xe-0/0/3, Enabled, Physical link is Up
- Interface index: 200, SNMP ifIndex: 577, Generation: 203
- Pad to minimum frame size: Disabled
- Device flags: Present Running
- Interface flags: SNMP-Traps Internal: 0x4000
- Link flags: None
- CoS queues: 8 supported, 8 maximum usable queues
- Schedulers: 0
- Hold-times: Up 0 ms, Down 0 ms
- Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
- Statistics last cleared: Never
- Traffic statistics:
  - Input bytes: 0
  - Output bytes: 0
  - Input packets: 0
  - Output packets: 0
- IPv6 transit statistics:
  - Input bytes: 0
  - Output bytes: 0
  - Input packets: 0
Output packets: 0
Dropped traffic statistics due to STP State:
  Input bytes: 0
  Output bytes: 0
  Input packets: 0
  Output packets: 0
  Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
  Output errors:
  Carrier transitions: 5, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 0 0 0
1 0 0 0
2 0 0 0
3 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
Active alarms: None
Active defects: None
PCS statistics: Seconds
  Bit errors 0
 Errored blocks 4
MAC statistics: Receive Transmit
  Total octets 0 0
  Total packets 0 0
  Unicast packets 0 0
  Broadcast packets 0 0
  Multicast packets 0 0
  CRC/Align errors 0 0
  FIFO errors 0 0
  MAC control frames 0 0
  MAC pause frames 0 0
  Oversized frames 0 0
  Jabber frames 0 0
  Fragment frames 0 0
  VLAN tagged frames 0 0
  Code violations 0 0
  Total errors 0 0
Filter statistics:
  Input packet count 0
  Input packet rejects 0
  Input DA rejects 0
  Input SA rejects 0
  Output packet count 0
  Output packet pad count 0
  Output packet error count 0
CAM destination filters: 0, CAM source filters: 0
Packet Forwarding Engine configuration:
show interfaces extensive (MX480 Router with MPC5E and 100-Gigabit Ethernet OTN Interface)

user@host> show interfaces et-2/1/0 extensive

Physical interface: et-2/1/0, Enabled, Physical link is Up
   Interface index: 215, SNMP ifIndex: 872, Generation: 218
   Pad to minimum frame size: Disabled
   Device flags : Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Link flags : None
   CoS queues : 8 supported, 8 maximum usable queues
   Schedulers : 0
   Hold-times : Up 0 ms, Down 0 ms
   Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
   Statistics last cleared: Never
   Traffic statistics:
      Input bytes : 0 0 bps
      Output bytes : 0 0 bps
      Input packets: 0 0 pps
      Output packets: 0 0 pps
   IPv6 transit statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Dropped traffic statistics due to STP State:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Input errors:
      Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
   Output errors:
      Carrier transitions: 263, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
   Egress queues: 8 supported, 4 in use

<table>
<thead>
<tr>
<th>Limit</th>
<th>%</th>
<th>bps</th>
<th>%</th>
<th>usec</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>95</td>
<td>9500000000</td>
<td>95</td>
<td>0</td>
<td>low</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>500000000</td>
<td>5</td>
<td>0</td>
<td>low</td>
</tr>
</tbody>
</table>

Interface transmit statistics: Disabled
<table>
<thead>
<tr>
<th>Queue number:</th>
<th>Mapped forwarding classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
</tr>
<tr>
<td>1</td>
<td>expedited-forwarding</td>
</tr>
<tr>
<td>2</td>
<td>assured-forwarding</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
</tr>
</tbody>
</table>

Active alarms: None
Active defects: None

PCS statistics

<table>
<thead>
<tr>
<th>Bit errors</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errored blocks</td>
<td>754</td>
</tr>
</tbody>
</table>

MAC statistics:

<table>
<thead>
<tr>
<th>Total octets</th>
<th>Receive</th>
<th>14960</th>
<th>Transmit</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total packets</td>
<td>104</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

MAC control frames

<table>
<thead>
<tr>
<th>MAC control frames</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total errors</td>
<td>98</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:

<table>
<thead>
<tr>
<th>Input packet count</th>
<th>104</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input packet rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input DA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Input SA rejects</td>
<td>0</td>
</tr>
<tr>
<td>Output packet count</td>
<td>0</td>
</tr>
<tr>
<td>Output packet pad count</td>
<td>0</td>
</tr>
<tr>
<td>Output packet error count</td>
<td>0</td>
</tr>
</tbody>
</table>

CAM destination filters: 0, CAM source filters: 0

OTN alarms: None
OTN defects: None
OTN FEC Mode: GFEC
OTN Rate: OTU4 100Gbps
OTN Line Loopback: None
OTN Local Loopback: None
OTN Payload PRBS: None

OTN FEC statistics:

| Corrected Errors | 169828399453 |
| Uncorrected Words | 28939961456 |
| Corrected Error Ratio (17963 sec average) | 8.46e-05 |

OTN FEC alarms:

<table>
<thead>
<tr>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEC Degrad</td>
<td>1180</td>
<td>3 OK</td>
</tr>
<tr>
<td>FEC Excessive</td>
<td>1160</td>
<td>5 OK</td>
</tr>
</tbody>
</table>

OTN OC:

<table>
<thead>
<tr>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOS</td>
<td>129</td>
<td>1 OK</td>
</tr>
<tr>
<td>LOF</td>
<td>2</td>
<td>1 OK</td>
</tr>
<tr>
<td>LOM</td>
<td>0</td>
<td>0 OK</td>
</tr>
<tr>
<td>Wavelength Lock</td>
<td>0</td>
<td>0 OK</td>
</tr>
</tbody>
</table>

OTN OTU:

| AIS | 0 | 0 OK |
| BDI | 7 | 1 OK |
IAE                          0            0  OK
TTIM                       168           45  OK
BIAE                         0            0  OK
TSF                           0           0  OK
SSF                           0           0  OK
Received DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Received SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Transmitted DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Transmitted SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
OTN ODU:
AIS                        130            1  OK
OCI                          0            0  OK
LCK                          0            0  OK
CSF                          8            4  OK
TSF                          0            0  OK
SSF                          0            0  OK
PTIM                       130            1  OK
Received DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Received SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Transmitted DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
Transmitted SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..................
OTN Received Overhead Bytes:
  APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
  Payload Type: 0x00
ODU Delay Management:
  Result : 0x00
PRBS:
  Result: Test not enabled
OTN Transmitted Overhead Bytes:
  APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
  Payload Type: 0x00
Packet Forwarding Engine configuration:
  Destination slot: 0 (0x00)
  CoS information:
    Direction : Output
    CoS transmit queue               Bandwidth   Buffer Priority
                              %            bps     %           usec
    Limit                  %            bps     %           usec
    none 0 best-effort   95 95000000000    95              0      low
    none
    3 network-control     5 50000000000      5              0      low
    none
Interface transmit statistics: Disabled
Physical interface: et-3/0/0, Enabled, Physical link is Up
Interface index: 163, SNMP ifIndex: 564, Generation: 166
Pad to minimum frame size: Disabled
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags : None
Wavelength : 1550.12 nm, Frequency: 193.40 THz
CoS queues : 8 supported, 8 maximum usable queues
Schedulers : 0
Hold-times : Up 0 ms, Down 0 ms
Damping : half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsuppressed
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped : 2016-02-17 14:26:31 PST (09:04:28 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Dropped traffic statistics due to STP State:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 5, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 0 0 0
1 0 0 0
2 0 0 0
3 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
Active alarms : None
Active defects : None

<table>
<thead>
<tr>
<th>PCS statistics</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit errors</td>
<td>8</td>
</tr>
<tr>
<td>Errored blocks</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC statistics:</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VLAN tagged frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total errors</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter statistics:
- Input packet count: 0
- Input packet rejects: 0
- Input DA rejects: 0
- Input SA rejects: 0

OTN alarms:
- OTN defects: None
- OTN FEC Mode: SDFEC
- OTN Rate: OTU4 (120.5Gbps)
- OTN Line Loopback: None
- OTN Local Loopback: None
- OTN Payload PRBS: None
- OTN Laser Enable: On

OTN FEC statistics:
- Corrected Errors: 7065332638
- Uncorrected Words: 3412572
- Corrected Error Ratio (32785 sec average): 1.79e-06 (INVALID)

OTN FEC alarms:
- FEC Degraded: 0
- FEC Excessive: 3

OTN OC:
- LOS: 3
- LOF: 50
- LOM: 3
- Wavelength Lock: 0

OTN OTU:
- AIS: 0
- BDI: 4
- IAE: 4
- TTIM: 1
- BIAE: 3
- TSF: 50
- SSF: 50

Received DAPI: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Received SAPI:
show interfaces extensive (PTX3000 Router with 5-port 100-Gigabit DWDM OTN PIC)

user@host > show interfaces extensive et-4/0/0

Physical interface: et-4/0/0, Enabled, Physical link is Up
  Interface index: 148, SNMP ifIndex: 544, Generation: 161
  Link-level type: Ethernet, MTU: 1514, Speed: 100Gbps, BPDU Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
Wavelength : 1550.12 nm, Frequency: 193.40 THz
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Damping     : half-life: 0 sec, max-suppress: 0 sec, reuse: 0, suppress: 0, state: unsuppressed
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped : 2016-06-04 21:42:42 PDT (1d 05:09 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:

<table>
<thead>
<tr>
<th>Queue number</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control
Active alarms : None
Active defects : None
PCS statistics

<table>
<thead>
<tr>
<th>Bit errors</th>
<th>Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

Errored blocks 10
MAC statistics:

<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
VLAN tagged frames                      0
Code violations                          0

Filter statistics:
  Input packet count                  0
  Input packet rejects                0
  Input DA rejects                    0
  Input SA rejects                    0
  Output packet count                0
  Output packet pad count             0
  Output packet error count           0
CAM destination filters: 0, CAM source filters: 0

OTN alarms                               : None
OTN defects                               : None
OTN FEC Mode                              : SDFEC
OTN Rate                                  : OTU4 (120.5Gbps)
OTN Line Loopback                         : None
OTN Local Loopback                        : None
OTN Payload PRBS                          : None
OTN Laser Enable                          : On

OTN FEC statistics:
  Corrected Errors                      19637746
  Uncorrected Words                     0
  Corrected Error Ratio (104923 sec average)  1.55e-09

OTN FEC alarms:
  FEC Degrade                           0 Seconds  0 Count  OK
  FEC Excessive                         0 Seconds  0 Count  OK

OTN OC:
  LOS                                    0 Seconds  0 Count  OK
  LOF                                    2 Seconds  1 Count  OK
  LOM                                    2 Seconds  1 Count  OK
  Wavelength Lock                        0 Seconds  0 Count  OK

OTN OTU:
  AIS                                    0 Seconds  0 Count  OK
  BDI                                    2 Seconds  1 Count  OK
  IAE                                    0 Seconds  0 Count  OK
  TTIM                                   0 Seconds  0 Count  OK
  BIAE                                   0 Seconds  0 Count  OK
  TSF                                    2 Seconds  1 Count  OK
  SSF                                    0 Seconds  0 Count  OK
Received DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... Received SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... Transmitted DAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... Transmitted SAPI:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .......... OTN ODU:
  AIS                                    0 Seconds  0 Count  OK
  OCI                                    0 Seconds  0 Count  OK
  LCK                                    0 Seconds  0 Count  OK
  BDI                                    2 Seconds  1 Count  OK
  TTIM                                   0 Seconds  0 Count  OK
  IAE                                    0 Seconds  0 Count  OK
  LTC                                    0 Seconds  0 Count  OK
  CSF                                    0 Seconds  0 Count  OK
  TSF                                    2 Seconds  1 Count  OK
  SSF                                    0 Seconds  0 Count  OK
  PTIM                                   2 Seconds  1 Count  OK
Received DAPI:
show interfaces extensive (MX2020 Router with MPC6E and OTN MIC)

user@host> show interfaces xe-3/0/0 extensive

  Physical interface: xe-3/0/0, Enabled, Physical link is Up
    Interface index: 166, SNMP ifIndex: 516, Generation: 169
    Link-level type: Ethernet, MTU: 1514, MRU: 1522, LAN-PHY mode, Speed: 10Gbps,
    BPDU Error: None, MAC-REWRITE Error: None, Loopback: None, Source filtering: Disabled, Flow
    control: Enabled
    Pad to minimum frame size: Disabled
    Device flags : Present Running
    Interface flags: SNMP-Traps Internal: 0x4000
    Link flags : None
    CoS queues : 8 supported, 8 maximum usable queues
    Hold-times : Up 0 ms, Down 0 ms
    Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
    Statistics last cleared: Never
    Traffic statistics:
      Input bytes : 0 0 bps
      Output bytes : 0 0 bps
      Input packets: 0 0pps
      Output packets: 0 0pps
    IPv6 transit statistics:
      Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Dropped traffic statistics due to STP State:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes:
0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0

Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-forwarding</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forwarding</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control

Active alarms : None
Active defects : None

PCS statistics
Bit errors 2
Errored blocks 2

MAC statistics:
MAC control frames 0 0
MAC pause frames 0 0
Oversized frames 0 0
Jabber frames 0 0
Fragment frames 0 0
VLAN tagged frames 0 0
Code violations 0 0
Total errors 0 0

FIFO errors 0 0

Filter statistics:
Input packet count 0
Input packet rejects 0
Input DA rejects 0
Input SA rejects 0
Output packet count 0
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output packet pad count</td>
<td>0</td>
</tr>
<tr>
<td>Output packet error count</td>
<td>0</td>
</tr>
<tr>
<td>CAM destination filters</td>
<td>0</td>
</tr>
<tr>
<td>CAM source filters</td>
<td>0</td>
</tr>
<tr>
<td>OTN alarms</td>
<td>None</td>
</tr>
<tr>
<td>OTN defects</td>
<td>None</td>
</tr>
<tr>
<td>OTN FEC Mode</td>
<td>GFEC</td>
</tr>
<tr>
<td>OTN Rate</td>
<td>11.0957Gbps</td>
</tr>
<tr>
<td>OTN Line Loopback</td>
<td>None</td>
</tr>
<tr>
<td>OTN Local Loopback</td>
<td>None</td>
</tr>
<tr>
<td>OTN Payload PRBS</td>
<td>None</td>
</tr>
<tr>
<td>OTN FEC statistics: Corrected Errors</td>
<td>0</td>
</tr>
<tr>
<td>OTN FEC alarms: FEC Degraded</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: LOS</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: LOF</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: LOM</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: Wavelength Lock</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: AIS</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: BDI</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: IAE</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: TTIM</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: BIAE</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: TSF</td>
<td>0</td>
</tr>
<tr>
<td>OTN OC: SSF</td>
<td>0</td>
</tr>
<tr>
<td>OTN OTU: AIS</td>
<td>0</td>
</tr>
<tr>
<td>OTN OTU: BDI</td>
<td>0</td>
</tr>
<tr>
<td>OTN OTU: IAE</td>
<td>0</td>
</tr>
<tr>
<td>OTN OTU: TTIM</td>
<td>0</td>
</tr>
<tr>
<td>OTN Received Overhead Bytes</td>
<td>APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00</td>
</tr>
</tbody>
</table>
Payload Type: 0x00
ODU Delay Management:
Result: 0x00
PRBS:
Result: Test not enabled
OTN Transmitted Overhead Bytes:
APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
Payload Type: 0x00
Packet Forwarding Engine configuration:
Destination slot: 0 (0x00)
CoS information:
Direction: Output
<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>%</td>
<td>bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>9500000000</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>5000000000</td>
</tr>
</tbody>
</table>
Interface transmit statistics: Disabled

show interfaces extensive (MX2010 Router with MPC6E and 100-Gigabit Ethernet OTN Interface)

user@host> show interfaces et-9/0/0 extensive
Physical interface: et-9/0/0, Enabled, Physical link is Up
Interface index: 196, SNMP ifIndex: 623, Generation: 199
Pad to minimum frame size: Disabled
Device flags: Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags: None
CoS queues: 8 supported, 8 maximum usable queues
Hold-times: Up 0 ms, Down 0 ms
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
Last flapped: 2014-06-26 18:18:34 PDT (04:17:07 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes: 0 0 bps
Output bytes: 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Dropped traffic statistics due to STP State:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue number</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Queue number: Mapped forwarding classes
- 0: best-effort
- 1: expedited-forwarding
- 2: assured-forwarding
- 3: network-control

Active alarms: None
Active defects: None

PCS statistics
- Bit errors: 0
- Errored blocks: 0

MAC statistics: Receive Transmit
- Total octets: 0
- Total packets: 0
- Unicast packets: 0
- Broadcast packets: 0
- Multicast packets: 0
- CRC/Align errors: 0
- FIFO errors: 0
- MAC control frames: 0
- MAC pause frames: 0
- Oversized frames: 0
- Jabber frames: 0
- Fragment frames: 0
- VLAN tagged frames: 0
- Code violations: 0
- Total errors: 0

Filter statistics:
- Input packet count: 0
- Input packet rejects: 0
- Input DA rejects: 0
- Input SA rejects: 0
- Output packet count: 0
- Output packet pad count: 0
- Output packet error count: 0
- CAM destination filters: 0, CAM source filters: 0

Packet Forwarding Engine configuration:
- Destination slot: 0 (0x00)

CoS information:
- Direction: Output
- CoS transmit queue FIFO

<table>
<thead>
<tr>
<th>Limit</th>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
<td>95</td>
<td>95</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Interface transmit statistics: Disabled
show interfaces extensive (MX2010 Router with MPC6E and 10-Gigabit Ethernet Interface)

user@host> show interfaces xe-6/1/0 extensive

Physical interface: xe-6/1/0, Enabled, Physical link is Up
  Interface index: 159, SNMP ifIndex: 603, Generation: 162
  Link-level type: Ethernet, MTU: 1514, MRU: 1522, LAN-PHY mode, Speed: 10Gbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: None, Source filtering:
  Disabled, Flow control: Enabled
  Pad to minimum frame size: Disabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Schedulers : 0
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  IPv6 transit statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Dropped traffic statistics due to STP State:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3
    incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0,
    Resource errors: 0
  Output errors:
    Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
    FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 0 0 0
    1 0 0 0
    2 0 0 0
    3 0 0 0
  Queue number: Mapped forwarding classes
    0 best-effort
    1 expedited-forwarding
    2 assured-forwarding
    3 network-control
  Active alarms : None
  Active defects : None
  PCS statistics Seconds

Copyright © 2019, Juniper Networks, Inc.
Bit errors                             0
Errored blocks                         1
MAC statistics:                      Receive         Transmit
Total octets                             0                0
Total packets                            0                0
Unicast packets                          0                0
Broadcast packets                        0                0
Multicast packets                        0                0
CRC/Align errors                         0                0
FIFO errors                              0                0
MAC control frames                       0                0
MAC pause frames                         0                0
Oversized frames                         0
Jabber frames                            0
Fragment frames                          0
VLAN tagged frames                       0
Code violations                          0
Total errors                             0                0
Filter statistics:
Input packet count                       0
Input packet rejects                     0
Input DA rejects                         0
Input SA rejects                         0
Output packet count                                       0
Output packet pad count                                   0
Output packet error count                                 0
CAM destination filters: 0, CAM source filters: 0
Packet Forwarding Engine configuration:
  Destination slot: 0 (0x00)
CoS information:
  Direction : Output
  CoS transmit queue | Bandwidth % | Buffer Priority
  Limit             %            bps     %           usec
  0 best-effort 95 9500000000 95              0      low
  none
  3 network-control 5 500000000 5              0      low
  none
Interface transmit statistics: Disabled

show interfaces extensive (T4000 Routers with Type 5 FPCs)

The output fields for the show interfaces interface extensive command remains the same for 12-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (PF-12XGE-SFP), 24-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (PF-24XGE-SFP), and 100-Gigabit Ethernet Type 5 PIC with CFP (PF-1CGE-CFP).

user@host> show interfaces xe-4/0/0 extensive

Physical interface: xe-4/0/0, Enabled, Physical link is Up
  Interface index: 200, SNMP ifIndex: 592, Generation: 203
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error:
  None, Loopback: None, Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags   : None
  CoS queues   : 8 supported, 8 maximum usable queues
  Hold-times   : Up 0 ms, Down 0 ms
  Damping      : half-life: 5 sec, max-suppress: 20 sec, reuse 1000, suppress:
**2000**, state: enabled  
Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00  
Last flapped: 2013-06-03 16:01:56 PDT (06:04:07 ago)  
Statistics last cleared: Never  
**Traffic statistics:**  
<table>
<thead>
<tr>
<th></th>
<th>Input bytes:</th>
<th>0</th>
<th>0 bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output bytes:</td>
<td>0</td>
<td>0 bps</td>
<td></td>
</tr>
<tr>
<td>Input packets:</td>
<td>0</td>
<td>0 pps</td>
<td></td>
</tr>
<tr>
<td>Output packets:</td>
<td>0</td>
<td>0 pps</td>
<td></td>
</tr>
</tbody>
</table>
**IPv6 transit statistics:**  
| Input bytes: | 0 |  
| Output bytes: | 0 |  
| Input packets: | 0 |  
| Output packets: | 0 |  
**Input errors:**  
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0  
**Output errors:**  
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0  
**Egress queues:** 8 supported, 4 in use  
**Queue counters:**  
<table>
<thead>
<tr>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forwarding</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**Queue number:**  
0 | best-effort |  
1 | expedited-forwarding |  
2 | assured-forwarding |  
3 | network-control |  
**Active alarms:** None  
**Active defects:** None  
**PCS statistics:**  
| Bit errors | 0 |  
| Errored blocks | 0 |  
**MAC statistics:**  
| Total octets | Receive | Transmit |  
| Total packets | 0 | 0 |  
| Unicast packets | 0 | 0 |  
| Broadcast packets | 0 | 0 |  
| Multicast packets | 0 | 0 |  
| CRC/Align errors | 0 | 0 |  
| FIFO errors | 0 | 0 |  
| MAC control frames | 0 | 0 |  
| MAC pause frames | 0 | 0 |  
| Oversized frames | 0 | 0 |  
| Jabber frames | 0 | 0 |  
| Fragment frames | 0 | 0 |  
| VLAN tagged frames | 0 | 0 |  
| Code violations | 0 | 0 |  
**Filter statistics:**  
| Input packet count | 0 |  
| Input packet rejects | 0 |
Packet Forwarding Engine configuration:
Destination slot: 0 (0x00)

CoS information:
Direction: Output
CoS transmit queue | Bandwidth | Buffer Priority | Limit
<table>
<thead>
<tr>
<th>%</th>
<th>bps</th>
<th>%</th>
<th>usec</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
<td>95</td>
<td>9500000000</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
<td>5</td>
<td>500000000</td>
</tr>
</tbody>
</table>

Preclassifier statistics:
Traffic Class | Received Packets | Transmitted Packets | Dropped Packets
real-time      | 0                | 0                   | 0
network-control | 0                | 0                   | 0
best-effort   | 0                | 0                   | 0

Interface transmit statistics: Disabled

show interfaces extensive (Aggregated Ethernet)

user@host> show interfaces ae0 extensive

Physical interface: ae0, Enabled, Physical link is Up
   Interface index: 199, SNMP ifIndex: 570, Generation: 202
   Link-level type: Ethernet, MTU: 1514, Speed: 2Gbps, BPDU Error: None,
   MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
   Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
   Device flags: Present Running
   Interface flags: SNMP-Traps Internal: 0x4000
   Current address: 00:00:5E:00:53:00, Hardware address: 00:00:5E:00:53:00
   Last flapped: 2012-06-06 23:33:03 PDT (00:00:58 ago)
   Statistics last cleared: Never
   Traffic statistics:
   Input bytes : 18532 1984 bps
   Output bytes : 0 0 bps
   Input packets: 158 2 pps
   Output packets: 0 0 pps
   IPv6 transit statistics:
   Input bytes : 0
   Output bytes : 0
   Input packets: 0
   Output packets: 0
   Dropped traffic statistics due to STP State:
   Input bytes : 0
   Output bytes : 0
   Input packets: 0
   Output packets: 0
   Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
   Resource errors: 0
   Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
   Ingress queues: 8 supported, 4 in use
   Queue counters: Queued packets Transmitted packets Dropped packets
<table>
<thead>
<tr>
<th>Queue</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>57</td>
<td>57</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>63605</td>
<td>63605</td>
<td>0</td>
</tr>
</tbody>
</table>

Queue number: Mapped forwarding classes
0 best-effort
1 expedited-forwarding
2 assured-forwarding
3 network-control

Logical interface ae0.0 (Index 331) (SNMP ifIndex 583) (Generation 142)
Flags: SNMP-Traps 0x4004000 Encapsulation: ENET2
Statistics
Bundle:
Input : 149 2 17416 1984
Output: 0 0 0 0
Link:
ge-3/2/5.0
Input : 90 1 10100 992
Output: 0 0 0 0
ge-3/3/9.0
Input : 59 1 7316 992
Output: 0 0 0 0
LACP info:
Port  Port priority identifier priority number
key
ge-3/2/5.0 Actor 100 00:00:00:00:00:01 127 1
1 ge-3/2/5.0 Partner 127 00:24:dc:98:67:c0 127 1 1
ge-3/3/9.0 Actor 100 00:00:00:00:00:01 127 2
1 ge-3/3/9.0 Partner 127 00:24:dc:98:67:c0 127 2 1
LACP Statistics: LACP Rx LACP Tx Unknown Rx Illegal Rx
ge-3/2/5.0 38 137 0 0
ge-3/3/9.0 36 139 0 0
Marker Statistics: Marker Rx Resp Tx Unknown Rx Illegal Rx
ge-3/2/5.0 0 0 0 0
ge-3/3/9.0 0 0 0 0
Protocol inet, MTU: 1500, Generation: 169, Route table: 0
Flags: Sendbcast-pkt-to-re
Addresses, Flags: Is-Preferred Is-Primary
| Destination: 1.1.1/24, Local: 1.1.1.2, Broadcast: 1.1.1.255, Generation: 153 |
| Protocol multiservice, MTU: Unlimited, Generation: 170, Route table: 0 |
| Flags: Is-Primary |
| Policer: Input: __default_arp_policer__ |
**show interfaces lsi (Label-Switched Interface)**

**Syntax**

```
show interfaces interface-type
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <routing-instance instance-name>
  <snmp-index snmp-index>
  <statistics>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Display status information about the specified label-switched interface (LSI).

**Options**

- `interface-type`—On most routers, the interface type is `lt-fpc/pic/port`.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `routing-instance instance-name`—(Optional) Display information for the specified routing instance.
- `snmp-index snmp-index`—(Optional) Display information for the specified SNMP index of the interface.

**Required Privilege**

View

**Related Documentation**

List of Sample Output:

- `show interfaces lsi extensive on page 1660`

**Output Fields**

Table 52 on page 1658 lists the output fields for the `show interfaces` (logical tunnel) 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>Physical Interface</td>
<td>Name of the physical interface.</td>
<td>All levels</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>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Logical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP if index</td>
<td>SNMP interface index number.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Rate of bytes received on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Rate of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Rate of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Rate of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the logical interface, such as iso, inet6, mpls.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the protocol family flags. Possible values are described in the “Family Flags” section under “Common Output Fields Description” on page 1152.</td>
<td>detail extensive none</td>
</tr>
</tbody>
</table>
Sample Output

show interfaces lsi extensive

user@host> show interfaces lsi extensive

<table>
<thead>
<tr>
<th>Physical interface: lsi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface lsi.84934656 (Index 363) (SNMP ifIndex 586) (Generation 194)</td>
</tr>
<tr>
<td>Flags: Up Point-To-Point SNMP-Traps 0x4000000 Encapsulation: LSI-NULL</td>
</tr>
<tr>
<td>Traffic statistics:</td>
</tr>
<tr>
<td>Input bytes : 0</td>
</tr>
<tr>
<td>Output bytes : 0</td>
</tr>
<tr>
<td>Input packets: 0</td>
</tr>
<tr>
<td>Output packets: 0</td>
</tr>
<tr>
<td>Local statistics:</td>
</tr>
<tr>
<td>Input bytes : 0</td>
</tr>
<tr>
<td>Output bytes : 0</td>
</tr>
<tr>
<td>Input packets: 0</td>
</tr>
<tr>
<td>Output packets: 0</td>
</tr>
<tr>
<td>Transit statistics:</td>
</tr>
<tr>
<td>Input bytes : 0 0 bps</td>
</tr>
<tr>
<td>Output bytes : 0 0 bps</td>
</tr>
<tr>
<td>Input packets: 0 0 pps</td>
</tr>
<tr>
<td>Output packets: 0 0 pps</td>
</tr>
<tr>
<td>Protocol vpls, MTU: Unlimited, Generation: 279, Route table: 10</td>
</tr>
</tbody>
</table>

| Logical interface lsi.84934657 (Index 366) (SNMP ifIndex 589) (Generation 197) |
| Flags: Up Point-To-Point SNMP-Traps 0x4000000 Encapsulation: LSI-NULL |
| Traffic statistics: |
| Input bytes : 0 |
| Output bytes : 0 |
| Input packets: 0 |
| Output packets: 0 |
| Local statistics: |
| Input bytes : 0 |
| Output bytes : 0 |
| Input packets: 0 |
| Output packets: 0 |
| Transit statistics: |
| Input bytes : 0 0 bps |
| Output bytes : 0 0 bps |
| Input packets: 0 0 pps |
| Output packets: 0 0 pps |
| Protocol vpls, MTU: Unlimited, Generation: 282, Route table: 10 |
show interfaces media

Syntax

show interfaces media

Release Information


Description

Display media-specific information about all configured network interfaces.

NOTE: show interfaces media lists details for all interfaces, whereas show interfaces media interface-name lists details only for the specified interface.

NOTE: For the QFX5200 line of switches, there are no validation checks for the supported values of the optical properties. You must ensure that you configure the correct values. The optical properties are supported only on 100 Gigabit Ethernet interface.

Options

This command has no options.

Additional Information

Output from both the show interfaces interface-name detail and the show interfaces interface-name extensive commands includes all the information displayed in the output from the show interfaces media command.

Required Privilege Level

view

List of Sample Output

show interfaces media (SONET/SDH) on page 1662
show interfaces media (MX Series Routers) on page 1662
show interfaces media (PTX Series Packet Transport Routers) on page 1663
show interfaces media (QFX5200 Line of Switches) on page 1663

Output Fields

The output from the show interfaces media command includes fields that display interface media-specific information. These fields are also included in the show interfaces interface-name command for each particular interface type, and the information provided in the fields is unique to each interface type.

One field unique to the show interfaces media command is interface-type errors (for example, SONET errors). This field appears for channelized E3, channelized T3,
channelized OC, E1, E3, SONET, T1, and T3 interfaces. The information provided in this output field is also provided in the output from the `show interfaces interface-name` command. (For example, for SONET interfaces, these fields are SONET section, SONET line, and SONET path). For a description of errors, see the chapter with the particular interface type in which you are interested.

Sample Output

**show interfaces media (SONET/SDH)**

The following example displays the output fields unique to the `show interfaces media` command for a SONET interface (with no level of output specified):

```plaintext
user@host> show interfaces media so-4/1/2
Physical interface: so-4/1/2, Enabled, Physical link is Up
   Interface index: 168, SNMP ifIndex: 495
   Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC48,
      Loopback: None, FCS: 16, Payload scrambler: Enabled
   Device flags : Present Running
   Interface flags: Point-To-Point SNMP-Traps 16384
   Link flags : Keepalives
      Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
      Keepalive: Input: 1783 (00:00:00 ago), Output: 1786 (00:00:08 ago)
   LCP state: Opened
   NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
      mpls: Not-configured
   CHAP state: Not-configured
   CoS queues     : 8 supported
   Input rate     : 0 bps (0 pps)
   Output rate    : 0 bps (0 pps)
   SONET alarms   : None
   SONET defects  : None
   SONET errors:
   Received path trace: routerb so-1/1/2
   Transmitted path trace: routera so-4/1/2
```

**show interfaces media (MX Series Routers)**

```plaintext
user@host> show interfaces media xe-0/0/0/0
Physical interface: xe-0/0/0, Enabled, Physical link is Up
   Interface index: 145, SNMP ifIndex: 592
   Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 10Gbps, BPDU Error:
      None,
   Loopback: None, Source filtering: Disabled, Flow control: Enabled
   Pad to minimum frame size: Enabled
   Device flags : Present Running
   Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
   Link flags : None
   CoS queues     : 8 supported, 8 maximum usable queues
   Last flapped   : 2013-10-26 03:20:40 test (1w6d 00:19 ago)
   Input rate     : 0 bps (0 pps)
   Output rate    : 0 bps (0 pps)
   Active alarms  : LINK
```
Active defects : LINK
PCS statistics                      Seconds
  Bit errors                            78
  Errored blocks                        78
MAC statistics:
  Input bytes: 0, Input packets: 0, Output bytes: 0, Output packets: 0
Filter statistics:
  Filtered packets: 0, Padded packets: 0, Output packet errors: 0
Interface transmit statistics: Disabled

show interfaces media (PTX Series Packet Transport Routers)
user@host> show interfaces media em0
Physical interface: em0, Enabled, Physical link is Up
  Interface index: 8, SNMP ifIndex: 0
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Current address: 00:80:f9:25:00:1b, Hardware address: 00:80:f9:25:00:1b
  Last flapped : Never
  Input packets : 215151
  Output packets: 72

show interfaces media (QFX5200 Line of Switches)
Physical interface: et-0/0/12, Enabled, Physical link is Up
  Interface index: 674, SNMP ifIndex: 531
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 100Gbps, BPDU Error: None, Loop Detect PDU Error: None, Ethernet-Switching Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Media type: Fiber
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags : None
  CoS queues : 10 supported, 10 maximum usable queues
  Last flapped : 2018-10-05 23:23:45 PDT (01:47:17 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  Active alarms : None
  Active defects : None
  Pre-emphasis(reg 236/237)
    Register-value                10
  Ctie(reg 234/235)
    Register-value                 0
  Differential-amplitude(reg 238/239)
    Register-value                 0
PCS statistics                      Seconds
  Bit errors                            0
  Errored blocks                        0
Ethernet FEC Mode :                  FEC91
Ethernet FEC statistics Errors
  FEC Corrected Errors                0
  FEC Uncorrected Errors              0
  FEC Corrected Errors Rate           0
  FEC Uncorrected Errors Rate         0
MAC statistics:
- Input bytes: 0, Input packets: 0, Output bytes: 0, Output packets: 0
- PRBS Statistics: Disabled
- Interface transmit statistics: Disabled
**show interfaces terse**

**Syntax**
```
show interfaces terse
```

**Release Information**
Command introduced before Junos OS Release 7.4.

**Description**
Display summary information about interfaces.

**Options**
This command has no options.

**Additional Information**
Interfaces are always displayed in numerical order, from the lowest to the highest FPC slot number. Within that slot, the lowest PIC slot is shown first. On an individual PIC, the lowest port number is always first.

**Required Privilege**
view

**Related Documentation**
- Setting Up Logical Systems

**List of Sample Output**
- show interfaces terse on page 1666
- show interfaces terse (TX Matrix Plus Router) on page 1666
- show interfaces terse (PTX Series Packet Transport Routers) on page 1667

**Output Fields**
Table 53 on page 1665 lists the output fields for the `show interfaces terse` command. Output fields are listed in the approximate order in which they appear.

**Table 53: show interfaces terse Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>Admin</td>
<td>Whether the interface is turned on (up) or off (down).</td>
</tr>
<tr>
<td>Link</td>
<td>Link state: up or down.</td>
</tr>
<tr>
<td>Proto</td>
<td>Protocol family configured on the logical interface. A logical interface on a router that supports Ethernet OAM always shows the multiservice protocol.</td>
</tr>
<tr>
<td>Local</td>
<td>Local IP address of the logical interface.</td>
</tr>
<tr>
<td>Remote</td>
<td>Remote IP address of the logical interface.</td>
</tr>
</tbody>
</table>
### Sample Output

#### `show interfaces terse`

```bash
user@host> show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1-0/1/0:0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t1-0/1/0:0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>192.168.220.18/30</td>
<td></td>
</tr>
<tr>
<td>t1-0/1/0:1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t1-0/1/0:2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t1-0/1/0:3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>at-1/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>at-1/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dsc</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fxp0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fxp0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>192.168.71.249/21</td>
<td></td>
</tr>
<tr>
<td>fxp1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fxp1.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.0.0.4/8</td>
<td>4</td>
</tr>
<tr>
<td>gre</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipip</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>127.0.0.1</td>
<td>--&gt; 0/0</td>
</tr>
<tr>
<td>lo0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>127.0.0.1</td>
<td>--&gt; 0/0</td>
</tr>
<tr>
<td>lsi</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mtun</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

#### `show interfaces terse (TX Matrix Plus Router)`

```bash
user@host> show interfaces terse

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-0/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-0/0/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-0/0/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/0/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/0/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/1/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/1/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/1/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-6/1/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>1.1.1.1/30</td>
<td></td>
</tr>
<tr>
<td>ge-1/3/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>--&gt; 0/0</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.1/30</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.1</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.5/30</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.2</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.9/30</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.3</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.13/30</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.4</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.17/30</td>
<td></td>
</tr>
<tr>
<td>ge-7/0/0.5</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>2.15.1.21/30</td>
<td></td>
</tr>
</tbody>
</table>
...
### show interfaces terse (PTX Series Packet Transport Routers)

```
user@host>  show interfaces em0 terse
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>em0</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td>inet 192.168.3.30/24</td>
<td></td>
</tr>
<tr>
<td>em0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gre</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipip</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ixgbe0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ixgbe0.0</td>
<td></td>
<td></td>
<td></td>
<td>inet 10.34.0.4/8 162.0.0.4/2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>inet6 fe80::200:ff:fe22:4/64 fec0::a:22:0:4/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>tnp 0x22000004</td>
<td></td>
</tr>
<tr>
<td>ixgbe1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ixgbe1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>inet 10.34.0.4/8 162.0.0.4/2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>inet6 fe80::200:1ff:fe22:4/64 fec0::a:22:0:4/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>tnp 0x22000004</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 15

ANCP Operational Commands

- clear ancp neighbor
- clear ancp statistics
- clear ancp subscriber
- request ancp oam interface
- request ancp oam neighbor
- show ancp cos
- show ancp neighbor
- show ancp statistics
- show ancp subscriber
- show ancp summary
- show ancp summary neighbor
- show ancp summary subscriber
clear ancp neighbor

Syntax

```
clear ancp neighbor
  <ip-address ip-address>
  <system-name mac-address>
```

Release Information

Command introduced in Junos OS Release 9.4.

Description

Clear the ANCP agent connection with all ANCP neighbors or with the specified ANCP neighbor. This command deletes information for subscribers associated with the neighbor, causing the adjusted traffic rates to revert to the configured rate for the subscriber interfaces. The neighbor remains configured (its administrative state is enabled) and can reestablish adjacencies.

This command initiates logout of ANCP-triggered dynamic VLAN sessions on the physical interface associated with the specified neighbor; conventionally autosensed dynamic VLAN sessions and their associated logical interfaces are not affected.

Options

- **none**—Clear all ANCP neighbors.
- **ip-address ip-address**—(Optional) Clear the ANCP neighbor specified by the IP address.
- **system-name mac-address**—(Optional) Clear the ANCP neighbor specified by the MAC address.

Required Privilege

```
clear
```

Related Documentation

- show ancp neighbor on page 1686

List of Sample Output

- clear ancp neighbor on page 1670
- show ancp neighbor on page 1671

Output Fields

When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbors to verify the clear operation.

Sample Output

```
clear ancp neighbor
```

```
user@host> clear ancp neighbor
```

Copyright © 2019, Juniper Networks, Inc.
**show ancp neighbor**

The following sample output displays the connections with ANCP neighbors before and after the `clear ancp neighbor` command was issued.

```
user@host> show ancp neighbor

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
<th>Subscriber Count</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.0.113.102</td>
<td>00:00:5e:00:53:10</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
<tr>
<td>203.0.113.122</td>
<td>00:00:5e:00:53:12</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
<tr>
<td>203.0.113.132</td>
<td>00:00:5e:00:53:13</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
<tr>
<td>203.0.113.142</td>
<td>00:00:5e:00:53:14</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
</tbody>
</table>

user@host> clear ancp neighbor ip-address 203.0.113.102

user@host> show ancp neighbor

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
<th>Subscriber Count</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>203.0.113.122</td>
<td>00:00:5e:00:53:12</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
<tr>
<td>203.0.113.132</td>
<td>00:00:5e:00:53:13</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
<tr>
<td>203.0.113.142</td>
<td>00:00:5e:00:53:14</td>
<td>Established</td>
<td>$</td>
<td>Topo</td>
</tr>
</tbody>
</table>
```
clear ancp statistics

Syntax

clear ancp statistics
<ip-address ip-address>
<system-name mac-address>

Release Information
Command introduced in Junos OS Release 13.3.

Description
Clear current statistics accumulated by the ANCP agent for all ANCP neighbors or the specified neighbor.

Options none—Clear all ANCP statistics.

ip-address ip-address—(Optional) Clear statistics for the ANCP neighbor specified by the IP address.

system-name mac-address—(Optional) Clear statistics for the ANCP neighbor specified by the MAC address.

Required Privilege
clear

Related Documentation
• show ancp neighbor on page 1686

List of Sample Output
clear ancp statistics on page 1672
show ancp neighbor on page 1672

Output Fields
When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbor statistics to verify the clear operation.

Sample Output

clear ancp statistics

user@host> clear ancp statistics

show ancp neighbor

The following sample output displays statistics for an ANCP neighbor before and after the clear ancp statistics command was issued.

user@host> show ancp neighbor ip-address 192.168.10.1 detail

Neighbor Information
IP Address : 192.168.10.1
System Name : 00:00:5E:00:53:02
Up Time : 38
TCP Port : 64959
State : Established
Subscriber Count : 7
Capabilities : Topology Discovery
System Instance : 11
Peer Instance : 1
Adjacency Timer (in 100ms) : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Dead Timer : 22
Received Syn Count : 47
Received Synack Count : 48
Received Rstack Count : 2
Received Ack Count : 12
Received Port Up Count : 8
Received Port Down Count : 2
Received Other Count : 0
Sent Syn Count : 48
Sent Synack Count : 47
Sent Rstack Count : 1
Sent Ack Count : 12
Max Discovery Limit Exceed Count : 0

user@host> clear ancp statistics ip-address 192.168.10.1

user@host> show ancp neighbor ip-address 192.168.10.1 detail

Neighbor Information
IP Address : 192.168.10.1
System Name : 00:00:5E:00:53:02
Up Time : 38
TCP Port : 64959
State : Established
Subscriber Count : 7
Capabilities : Topology Discovery
System Instance : 11
Peer Instance : 1
Adjacency Timer (in 100ms) : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Dead Timer : 22
Received Syn Count : 47
Received Synack Count : 48
Received Rstack Count : 2
Received Ack Count : 12
Received Port Up Count : 8
Received Port Down Count : 2
Received Other Count : 0
Sent Syn Count : 48
Sent Synack Count : 47
Sent Rstack Count : 1
Sent Ack Count : 12
Max Discovery Limit Exceed Count : 0
Max Discovery Limit Exceed Count  : 0
**clear ancp subscriber**

**Syntax**

```plaintext
clear ancp subscriber
<identifier identifier>
<ip-address ip-address>
<system-name mac-address>
```

**Release Information**

Command introduced in Junos OS Release 11.4.

**Description**

Clear the ANCP agent connection with all ANCP subscribers or with the specified ANCP subscriber. This command deletes information for the subscribers, causing the adjusted traffic rate to revert to the configured rate for the subscriber interface, but otherwise has no affect on ANCP neighbors.

**Options**

- **none**—Clear all ANCP subscribers.
- **identifier identifier-string**—(Optional) Clear the ANCP subscriber identified by the access loop ID.
- **ip-address ip-address**—(Optional) Clear all ANCP subscribers on the neighbor specified by the IP address.
- **system-name mac-address**—(Optional) Clear all ANCP subscribers on the neighbor specified by the MAC address.

**Required Privilege Level**

clear

**Related Documentation**

- show ancp subscriber on page 1699

**List of Sample Output**

show ancp subscriber brief on page 1675

**Output Fields**

When you enter this command, you are provided no feedback on the status of your request. You can enter the `show ancp subscriber` command before and after clearing the ANCP neighbors to verify the clear operation.

**Sample Output**

show ancp subscriber brief

```
user@host> show ancp subscriber brief

<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>Type</th>
<th>Interface</th>
<th>Rate</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-1-10</td>
<td>VDSL2</td>
<td>set-ge-10410</td>
<td>64</td>
<td>203.0.113.102</td>
</tr>
<tr>
<td>port-1-11</td>
<td>VDSL2</td>
<td>set-ge-10411</td>
<td>64</td>
<td>203.0.113.112</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>Type</th>
<th>Interface</th>
<th>Rate</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-2-10</td>
<td>VDSL2</td>
<td>ge-1/0/4.12</td>
<td>64</td>
<td>203.0.113.122</td>
</tr>
<tr>
<td>port-2-10</td>
<td>VDSL2</td>
<td>ge-1/0/4.12</td>
<td>64</td>
<td>203.0.113.123</td>
</tr>
<tr>
<td>port-2-11</td>
<td>VDSL2</td>
<td>ge-1/0/4.13</td>
<td>64</td>
<td>203.0.113.132</td>
</tr>
</tbody>
</table>

user@host> clear ancp subscriber identifier port-2-10

user@host> show ancp subscriber brief

<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>Type</th>
<th>Interface</th>
<th>Rate</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-1-10</td>
<td>VDSL2</td>
<td>set-ge-10410</td>
<td>64</td>
<td>203.0.113.102</td>
</tr>
<tr>
<td>port-1-11</td>
<td>VDSL2</td>
<td>set-ge-10411</td>
<td>64</td>
<td>203.0.113.112</td>
</tr>
<tr>
<td>port-2-11</td>
<td>VDSL2</td>
<td>ge-1/0/4.13</td>
<td>64</td>
<td>203.0.113.132</td>
</tr>
</tbody>
</table>

clear ancp subscriber

user@host> clear ancp subscriber
**request ancp oam interface**

**Syntax**
```
request ancp oam interface
(interface-name | interface-set set-name)
<count count>
<timeout duration>
```

**Release Information**
Command introduced in Junos OS Release 11.4.

**Description**
Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify either an ANCP interface or an ANCP interface set. The access node responds to the NAS with the results of the test.

**Options**
- `interface-name`—Name of the ANCP interface on whose local loop the loopback test is run.
- `interface-set set-name`—Name of the ANCP interface set on whose local loop the loopback test is run.
- `count count`—(Optional) Number of times a loopback message is sent on the local loop. Range: 1 through 32. Default: 1.
- `timeout duration`—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request. Range: 0 through 255. Default: 5.

**Required Privilege Level**
view

**Related Documentation**
- Triggering ANCP OAM to Test the Local Loop

**List of Sample Output**
request ancp oam interface on page 1677

**Output Fields**
When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

**Sample Output**
```
request ancp oam interface
user@host> request ancp oam interface ge-1/0/4.12 count 5 timeout 40
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
```
request ancp oam neighbor

Syntax
request ancp oam neighbor
(ip-address ip-address | system-name neighbor-name)
subscriber identifier-string
<count count>
<timeout duration>

Release Information
Command introduced in Junos OS Release 11.4.

Description
Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify both the access node and the subscriber. The access node responds to the NAS with the results of the test.

Options
ip-address ip-address—IP address that specifies the access node on whose local loop the loopback test is run.

system-name neighbor-name—System name that specifies the access node on whose local loop the loopback test is run.

subscriber identifier-string—Access identifier that specifies the subscriber on whose local loop the loopback test is run.

count count—(Optional) Number of times a loopback message is sent on the local loop.
Range: 1 through 32. Default: 1.

timeout duration—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request.
Range: 0 through 255. Default: 5.

Required Privilege
view

Level

Related Documentation
• Triggering ANCP OAM to Test the Local Loop

List of Sample Output
request ancp oam subscriber on page 1679

Output Fields
When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

Sample Output
request ancp oam subscriber

user@host> request ancp oam neighbor 203.0.113.21 subscriber "dslam port-1-11"
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
show ancp cos

Syntax

show ancp cos
<identifier identifier>
<last-update>
<pending-update>

Release Information

Command introduced in Junos OS Release 9.4.

Description

Display information about the CoS state for subscriber traffic.

Options

identifier identifier—(Optional) Display information about the local loops for the specified access identifier.

last-update—(Optional) Display the most recently updated CoS information.

pending-update—(Optional) Display the pending update of CoS information.

Required Privilege

Level

view

Related Documentation

- show ancp neighbor on page 1686
- show ancp statistics on page 1694
- show ancp subscriber on page 1699

List of Sample Output

- show ancp cos on page 1683
- show ancp cos last-update on page 1684
- show ancp cos pending-update on page 1685

Output Fields

Table 54 on page 1681 lists the output fields for the show ancp cos command. Output fields are listed in the approximate order in which they appear.

**Table 54: show ancp cos Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-DSL CoS adjustment</td>
<td>Adjustment values applied by the ANCP agent to the actual downstream rates and frame overhead for frame-mode DSL types. The agent then reports the adjusted rates to CoS to establish a shaping rate for the CoS node that corresponds to the subscriber access line.</td>
</tr>
<tr>
<td>QoS Adjust Flag</td>
<td>State of QoS adjust:</td>
</tr>
<tr>
<td></td>
<td>• TRUE—The ANCP agent is enabled to adjust the actual downstream data rates and frame overhead and report the adjusted values to CoS.</td>
</tr>
<tr>
<td></td>
<td>• FALSE—The ANCP agent is not enabled to adjust and report values to CoS.</td>
</tr>
</tbody>
</table>
Table 54: show ancp cos Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL bytes</td>
<td>Number of bytes by which the actual ADSL downstream cell overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>ADSL2 bytes</td>
<td>Number of bytes by which the actual ADSL2 downstream cell overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>ADSL2-PLUS bytes</td>
<td>Number of bytes by which the actual ADSL2+ downstream cell overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>SDSL overhead adjusted</td>
<td>Percentage by which the actual SDSL downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to CoS.</td>
</tr>
<tr>
<td>SDSL bytes</td>
<td>Number of bytes by which the actual SDSL downstream frame overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>OTHER overhead adjusted</td>
<td>Percentage by which the actual OTHER downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to CoS.</td>
</tr>
<tr>
<td>OTHER bytes</td>
<td>Number of bytes by which the actual OTHER downstream frame overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>VDSL overhead adjusted</td>
<td>Percentage by which the actual VDSL downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to CoS.</td>
</tr>
<tr>
<td>VDSL bytes</td>
<td>Number of bytes by which the actual VDSL downstream frame overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>VDSL2 overhead adjusted</td>
<td>Percentage by which the actual VDSL2 downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to CoS.</td>
</tr>
<tr>
<td>VDSL2 bytes</td>
<td>Number of bytes by which the actual VDSL2 downstream frame overhead is adjusted</td>
</tr>
<tr>
<td></td>
<td>before reporting it to CoS.</td>
</tr>
<tr>
<td>Per-DSL adjustment for reporting</td>
<td>Adjustment values applied by the ANCP agent to the actual downstream rates for</td>
</tr>
<tr>
<td></td>
<td>individual DSL types to account for traffic overhead. The agent then reports</td>
</tr>
<tr>
<td></td>
<td>the adjusted rates to AAA.</td>
</tr>
<tr>
<td>ADSL adjustment factor</td>
<td>Percentage by which the actual ADSL downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to AAA.</td>
</tr>
<tr>
<td>ADSL2 adjustment factor</td>
<td>Percentage by which the actual ADSL2 downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to AAA.</td>
</tr>
<tr>
<td>ADSL2+ adjustment factor</td>
<td>Percentage by which the actual ADSL2+ downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to AAA.</td>
</tr>
<tr>
<td>VDSL adjustment factor</td>
<td>Percentage by which the actual VDSL downstream rate is adjusted before</td>
</tr>
<tr>
<td></td>
<td>reporting it to AAA.</td>
</tr>
</tbody>
</table>
### Table 54: `show ancp cos` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDSL2 adjustment factor</td>
<td>Percentage by which the actual VDSL2 downstream rate is adjusted before reporting it to AAA.</td>
</tr>
<tr>
<td>SDSL adjustment factor</td>
<td>Percentage by which the actual SDSL downstream rate is adjusted before reporting it to AAA.</td>
</tr>
<tr>
<td>OTHER adjustment factor</td>
<td>Percentage by which the actual OTHER downstream rate is adjusted before reporting it to AAA.</td>
</tr>
<tr>
<td>Keepalive Timer</td>
<td>Interval between the keepalive messages that the ANCP agent sends to CoS.</td>
</tr>
<tr>
<td>Cos State</td>
<td>State of the interaction between the ANCP agent and CoS:</td>
</tr>
<tr>
<td></td>
<td>• ANCPD_COS_CONNECT_NEEDED</td>
</tr>
<tr>
<td></td>
<td>• ANCPD_COS_CONNECT_PENDING</td>
</tr>
<tr>
<td></td>
<td>• ANCPD_COS_CONNECT_DONE</td>
</tr>
<tr>
<td></td>
<td>• ANCPD_COS_SESSION_SENT</td>
</tr>
<tr>
<td></td>
<td>• ANCPD_COS_WRITE_READY</td>
</tr>
<tr>
<td>Connect Time</td>
<td>Time at which the ANCP agent connected to CoS; useful for debugging.</td>
</tr>
<tr>
<td>Session Time</td>
<td>Time at which the ANCP agent sent a session connect message to CoS; useful for debugging.</td>
</tr>
<tr>
<td>Routing Instance Time</td>
<td>Time at which the ANCP agent sent the routing instance to CoS; useful for debugging.</td>
</tr>
<tr>
<td>Keepalive Time</td>
<td>Time at which the last keepalive message was sent.</td>
</tr>
<tr>
<td>Update Time</td>
<td>Time at which the shaping rate was last updated.</td>
</tr>
<tr>
<td>Type</td>
<td>Subscriber access type: ifl indicates that a single VLAN carries subscriber traffic and iflset indicates that a set of VLANs carries subscriber traffic.</td>
</tr>
<tr>
<td>Name</td>
<td>System-wide name of the particular subscriber access.</td>
</tr>
<tr>
<td>Index</td>
<td>Access identifier.</td>
</tr>
<tr>
<td>Pending Update</td>
<td>Actual downstream data rate to be applied next to this local loop, in Kbps.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Adjusted downstream data rate last reported to CoS by the ANCP agent for this local loop, in Kbps.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show ancp cos

user@host> show ancp cos
```
Per-DSL CoS adjustment:
Qos Adjust Flag: TRUE
ADSL bytes: 20
ADSL2 bytes: 20
ADSL2-PLUS bytes: 20
VDSL overhead adjusted: 90
VDSL bytes: 20
VDSL2 overhead adjusted: 95
VDSL2 bytes: -20
SDSL overhead adjusted: 85
SDSL bytes: 30
OTHER overhead adjusted: 85
OTHER bytes: 30

Per-DSL adjustment for reporting:
ADSL adjustment factor: 100
ADSL2 adjustment factor: 100
ADSL2+ adjustment factor: 100
VDSL adjustment factor: 100
VDSL2 adjustment factor: 100
SDSL adjustment factor: 100
OTHER adjustment factor: 100

Keepalive Timer: 45 secs
State: WRITE_READY
Connect Time: Fri May 2 12:08:49 2016
Session Time: Fri May 2 12:18:52 2016
Update Time: Fri May 2 13:02:55 2016

+-----------------+-----------------+-----------------+-----------------+-----------------+
<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Index</th>
<th>Pending Update</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>iflset</td>
<td>aci-1004-ge-2/0/0.1073741834</td>
<td>4</td>
<td>None</td>
<td>36000 Kbps</td>
</tr>
</tbody>
</table>
+-----------------+-----------------+-----------------+-----------------+-----------------+

show ancp cos last-update

Per-DSL CoS adjustment:
Qos Adjust Flag: TRUE
ADSL bytes: 20
ADSL2 bytes: 20
ADSL2-PLUS bytes: 20
VDSL overhead adjusted: 90
VDSL bytes: 20
VDSL2 overhead adjusted: 95
VDSL2 bytes: -20
SDSL overhead adjusted: 85
SDSL bytes: 30
OTHER overhead adjusted: 85
OTHER bytes: 30

Per-DSL adjustment for reporting:
ADSL adjustment factor: 100
ADSL2 adjustment factor: 100
ADSL2+ adjustment factor: 100
VDSL adjustment factor: 100
VDSL2 adjustment factor: 100

Copyright © 2019, Juniper Networks, Inc.
show ancp cos pending-update

user@host> show ancp cos pending-update

Per-DSL CoS adjustment:
  Qos Adjust Flag: TRUE
  VDSL overhead adjusted: 90
  VDSL bytes: 20
  VDSL2 overhead adjusted: 95
  VDSL2 bytes: -20
  SDSL overhead adjusted: 85
  SDSL bytes: 30
  OTHER overhead adjusted: 85
  OTHER bytes: 30

Per-DSL adjustment for reporting:
  ADSL adjustment factor: 100
  ADSL2 adjustment factor: 100
  ADSL2+ adjustment factor: 100
  VDSL adjustment factor: 100
  VDSL2 adjustment factor: 100
  SDSL adjustment factor: 100
  OTHER adjustment factor: 100

Keepalive Timer: 45 secs
State: WRITE_READY
Connect Time: Fri May 2 12:08:49 2016
Session Time: Fri May 2 12:18:52 2016
Keepalive Time: Fri May 2 13:44:34 2016
Update Time: Fri May 2 13:02:55 2016
**show ancp neighbor**

**Syntax**

```
show ancp neighbor
  <brief | detail>
  <ip-address ip-address>
  <system-name mac-address>
```

**Release Information**

Command introduced in Junos OS Release 9.4.

**Description**

Display information about all ANCP neighbors or the specified ANCP neighbor, regardless of operational state.

**Options**

- `brief | detail`—(Optional) Display the specified level of detail.
- `ip-address ip-address`—(Optional) Display information about the neighbor (access node) specified by the IP address.
- `system-name mac-address`—(Optional) Display information about the neighbor (access node) specified by the MAC address.

**Required Privilege Level**

```
view
```

**Related Documentation**

- show ancp cos on page 1681
- show ancp subscriber on page 1699

**List of Sample Output**

show ancp neighbor on page 1689
show ancp neighbor detail on page 1690
show ancp neighbor ip-address on page 1691
show ancp neighbor system-name on page 1692

**Output Fields**

Table 55 on page 1686 lists the output fields for the `show ancp neighbor` command. Output fields are listed in the approximate order in which they appear.

**Table 55: show ancp neighbor Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the ANCP implementation:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>- <strong>0x31</strong>—General Switch Management Protocol (GSMP) version 3, sub-version 1;</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>ANCP version before RFC 6320, *Protocol for Access Node Control Mechanism in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Broadband Networks*.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>0x32</strong>—ANCP version 1, defined in RFC 6320, *Protocol for Access Node Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mechanism in Broadband Networks*.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 55: show ancp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the ANCP neighbor.</td>
<td>brief detail</td>
</tr>
<tr>
<td>PartId</td>
<td>Number that associates the ANCP message with a specific partition.</td>
<td>brief none</td>
</tr>
<tr>
<td>State</td>
<td>Operational state of the ANCP adjacency:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Configured—The neighbor has been configured, but has never been in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Established state. An asterisk (*) is prefixed to the neighbor entry for this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Establishing—Adjacency negotiations are in progress for the neighbor. An asterisk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(*) is prefixed to the neighbor entry for this state. This state is rarely seen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>because the adjacency is established so quickly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Established—Adjacency negotiations have succeeded for the neighbor and an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ANCP session has been established.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not Established—Not Established; adjacency negotiations are ready to begin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that this neighbor previously had been in the Established state;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that is, it has lost a previously established adjacency. An asterisk (*) is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefixed to the neighbor entry for this state.</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>How long the adjacency has been up in one of the following formats:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>• nwndnh—number of weeks, days, and hours</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• nd hh:mm:ss—number of days, hours, minutes, and seconds</td>
<td></td>
</tr>
<tr>
<td>Subscriber Count</td>
<td>Number of subscribers associated with the ANCP neighbor (access local loop).</td>
<td>brief none</td>
</tr>
<tr>
<td>Capabilities</td>
<td>Negotiated ANCP capability:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Topo—Topology discovery.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OAM—Performance of local Operations Administration Maintenance (OAM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>procedures on an access loop controlled by the router.</td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>MAC address of the ANCP neighbor.</td>
<td>detail</td>
</tr>
<tr>
<td>TCP Port</td>
<td>TCP port on which ANCP messages are exchanged.</td>
<td>detail</td>
</tr>
<tr>
<td>System Instance</td>
<td>Number identifying the ANCP link instance from the edge device's perspective.</td>
<td>detail</td>
</tr>
<tr>
<td>Peer Instance</td>
<td>Number identifying the ANCP instance from the access node's perspective. This</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>number is unique and changes when the node or link comes back up after going</td>
<td></td>
</tr>
<tr>
<td></td>
<td>down.</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>Adjacency timer value advertised by the ANCP peer in 100 ms increments; the</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>interval between ANCP ACK messages. This value remains constant for the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>duration of an ANCP session.</td>
<td></td>
</tr>
</tbody>
</table>
Table 55: show ancp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Type</td>
<td>Number that identifies whether partitions are used and how the ID is negotiated:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 0—No partition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1—Fixed partition requested.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Fixed partition assigned.</td>
<td></td>
</tr>
<tr>
<td>Partition Flag</td>
<td>Number that specifies the type of partition requested: 1 (new adjacency) or 2</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>(recovered adjacency).</td>
<td></td>
</tr>
<tr>
<td>Partition Identifier</td>
<td>Number that identifies a logical partition of an access node with which the ANCP</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>agent has formed an adjacency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A value of zero indicates that the agent supports each neighbor on an IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>over a single TCP session with a partition ID of zero. This is the default support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>case.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A nonzero value indicates that the agent supports each neighbor on an IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>over a single TCP session with a nonzero partition ID.</td>
<td></td>
</tr>
<tr>
<td>Partition Adjacencies</td>
<td>Number of adjacencies that share the partition.</td>
<td>detail</td>
</tr>
<tr>
<td>Dead Timer</td>
<td>Remaining period that the edge device waits for adjacency packets from a neighbor</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>before declaring the neighbor to be down. The maximum dead time value is three</td>
<td></td>
</tr>
<tr>
<td></td>
<td>times the configured adjacency timer value. This field displays the current value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>based on the time that the last adjacency packet was received.</td>
<td></td>
</tr>
<tr>
<td>Received Syn Count</td>
<td>Number of synchronization messages received from neighbors to maintain adjacencies.</td>
<td>detail</td>
</tr>
<tr>
<td>Received Synack Count</td>
<td>Number of synchronization acknowledgment messages received from neighbors</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>in response to the node’s synchronization messages.</td>
<td></td>
</tr>
<tr>
<td>Received Rstack Count</td>
<td>Number of messages received from neighbors indicating that the link to the</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>neighbor needs to be reset.</td>
<td></td>
</tr>
<tr>
<td>Received Ack Count</td>
<td>Number of acknowledgment messages periodically received from neighbors after an</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>adjacency has been established.</td>
<td></td>
</tr>
<tr>
<td>Received Port Up Count</td>
<td>Number of status messages received from neighbors indicating that a port has</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>transitioned to the up state.</td>
<td></td>
</tr>
<tr>
<td>Received Port Down Count</td>
<td>Number of status messages received from neighbors indicating that a port has</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>transitioned to the down state.</td>
<td></td>
</tr>
<tr>
<td>Received Generic Resp Count</td>
<td>Number of generic response messages received from neighbors.</td>
<td>detail</td>
</tr>
<tr>
<td>Received Adjacency Update Count</td>
<td>Number of adjacency update messages received from neighbors.</td>
<td>detail</td>
</tr>
<tr>
<td>Received OAM Count</td>
<td>Number of OAM responses received from neighbors in reply to request commands.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 55: show ancp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Other Count</td>
<td>Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent Syn Count</td>
<td>Number of synchronization messages sent to neighbors to maintain adjacencies.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent Synack Count</td>
<td>Number of synchronization acknowledgment messages sent to neighbors in response to their synchronization messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent Rstack Count</td>
<td>Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent Ack Count</td>
<td>Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent Generic Resp Count</td>
<td>Number of generic response messages sent to neighbors.</td>
<td>detail</td>
</tr>
<tr>
<td>Sent OAM Count</td>
<td>Number of OAM request commands sent to neighbors.</td>
<td>detail</td>
</tr>
<tr>
<td>Max Discovery Limit Exceed Count</td>
<td>Number of times that the maximum number of discovery table entries accepted from the neighbor has been exceeded.</td>
<td>detail</td>
</tr>
<tr>
<td>Result Codes</td>
<td>Number of generic response messages sent to neighbors that include each of the following result codes:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>- <strong>Invalid Request Message Count</strong>—A properly formed request message violated the protocol because of timing (such as a race condition) or direction of transmission.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Specified Port(s) Down Count</strong>—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Out of Resources Count</strong>—ANCP is out of resources, probably not related to the access lines. This result code is sent only by an access node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Request Msg Not Implemented Count</strong>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Malformed Msg Count</strong>—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>TLV Missing Count</strong>—One or more mandatory TLVs was missing from a request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Invalid TLV Contents Count</strong>—The contents of one or more TLVs in the request do not match its required specification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Non-Existent Port(s) Count</strong>—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

```
show ancp neighbor
```

```
user@host> show ancp neighbor

<table>
<thead>
<tr>
<th>Version</th>
<th>IP Address</th>
<th>Capabilities</th>
<th>PartID</th>
<th>State</th>
<th>Time</th>
<th>Subscriber Count</th>
</tr>
</thead>
</table>
```
### show ancp neighbor detail

```
user@host> show ancp neighbor detail

Neighbor Information

| Version | IP Address  | System Name | Up Time | TCP Port | State       | Subscriber Count | Capabilities | System Instance | Peer Instance | Adjacency Timer (in 100ms) | Peer Adjacency Timer (in 100ms) | Partition Type | Partition Flag | Partition Identifier | Partition Adjacencies | Dead Timer | Received Syn Count | Received Synack Count | Received Rstack Count | Received Ack Count | Received Port Up Count | Received Port Down Count | Received Generic Resp Count | Received Adjacency Update Count | Received OAM Count | Received Other Count | Sent Syn Count | Sent Sync Count | Sent Rstack Count | Sent Ack Count | Sent Generic Resp Count | Sent OAM Count | Max Discovery Limit Exceed Count |
|---------|-------------|-------------|---------|----------|-------------|------------------|-----------------|-----------------|-----------------|-----------------|-----------------------------|-----------------------------|----------------|--------------|------------------|------------------|-------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| 0x31    | 203.0.113.13| 0           | Established | 11:24   | 2            | Topo             |                 |                 |                 |                 |                            |                            |                |              |                  |                  |             |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |
| 0x31    | 203.0.113.15| 0           | Not Establshd | 2:45    | 2            | Topo             |                 |                 |                 |                 |                            |                            |                |              |                  |                  |             |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |
| * 0x0   | 198.51.100.102| 0       | Establishing | 0       | 0            |                 |                 |                 |                 |                 |                            |                            |                |              |                  |                  |             |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |
| * 0x0   | 192.0.2.0    | 0           | Configured  | 0       | 0            |                 |                 |                 |                 |                 |                            |                            |                |              |                  |                  |             |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |
| * 0x0   | 192.0.2.1    | 0           | Configured  | 0       | 0            |                 |                 |                 |                 |                 |                            |                            |                |              |                  |                  |             |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |                 |
```

<table>
<thead>
<tr>
<th>Version</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x32</td>
<td>192.168.9.1</td>
</tr>
</tbody>
</table>

---

Copyright © 2019, Juniper Networks, Inc.
### show ancp neighbor ip-address

```
user@host> show ancp neighbor ip-address 192.0.2.85
```

<table>
<thead>
<tr>
<th>Neighbor Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td>0x32</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>192.0.2.85</td>
</tr>
<tr>
<td><strong>System Name</strong></td>
<td>00:00:5e:00:53:ba</td>
</tr>
<tr>
<td><strong>Up Time</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>TCP Port</strong></td>
<td>32666</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Established</td>
</tr>
<tr>
<td><strong>Subscriber Count</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td>Topo</td>
</tr>
<tr>
<td><strong>System Instance</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Peer Instance</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>Adjacency Timer (in 100ms)</strong></td>
<td>100</td>
</tr>
<tr>
<td><strong>Peer Adjacency Timer (in 100ms)</strong></td>
<td>100</td>
</tr>
</tbody>
</table>

### System Information

<table>
<thead>
<tr>
<th>System Name</th>
<th>00:00:5e:00:53:02</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Up Time</strong></td>
<td>36</td>
</tr>
<tr>
<td><strong>TCP Port</strong></td>
<td>61408</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Not Established</td>
</tr>
<tr>
<td><strong>Subscriber Count</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td>Topology Discovery</td>
</tr>
<tr>
<td><strong>System Instance</strong></td>
<td>12</td>
</tr>
<tr>
<td><strong>Peer Instance</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Adjacency Timer (in 100ms)</strong></td>
<td>50</td>
</tr>
<tr>
<td><strong>Peer Adjacency Timer (in 100ms)</strong></td>
<td>100</td>
</tr>
<tr>
<td><strong>Partition Type</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Partition Flag</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Partition Identifier</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Partition Adjacencies</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Dead Timer</strong></td>
<td>23</td>
</tr>
<tr>
<td><strong>Received Syn Count</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>Received Synack Count</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>Received Rstack Count</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Received Ack Count</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Received Port Up Count</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Received Port Down Count</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Received Generic Resp Count</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Received Adjacency Update Count</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Received OAM Responses Count</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Received Other Count</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Sent Syn Count</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>Sent Synack Count</strong></td>
<td>24</td>
</tr>
<tr>
<td><strong>Sent Rstack Count</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Sent Generic Resp Count</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Sent Ack Count</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Sent OAM Requests Count</strong></td>
<td>4</td>
</tr>
<tr>
<td><strong>Max Discovery Limit Exceed Count</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

### Result Codes

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Request Message Count</td>
<td>0</td>
</tr>
<tr>
<td>Specified Port(s) Down Count</td>
<td>0</td>
</tr>
<tr>
<td>Out of Resources Count</td>
<td>0</td>
</tr>
<tr>
<td>Request Msg Not Implemented Count</td>
<td>0</td>
</tr>
<tr>
<td>Malformed Msg Count</td>
<td>0</td>
</tr>
<tr>
<td>TLV Missing Count</td>
<td>0</td>
</tr>
<tr>
<td>Invalid TLV Contents Count</td>
<td>0</td>
</tr>
<tr>
<td>Non-Existent Port(s) Count</td>
<td>0</td>
</tr>
</tbody>
</table>
show ancp neighborsystem-name

user@host> show ancp neighbor 00:00:5e:00:53:ba detail

Neighbor Information
Version : 0x31
IP Address : 203.0.113.101
System Name : 00:00:5e:00:53:ba
Up Time : 19
TCP Port : 1028
State : Established
Subscriber Count : 2
Capabilities : Topology Discovery, OAM
System Instance : 1
Peer Instance : 10
Adjacency Timer (in 100ms) : 100
Peer Adjacency Timer (in 100ms) : 250
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer : 55
Received Syn Count : 1
Received Synack Count : 1
Received Rstack Count : 0
Received Ack Count : 4
Received Port Up Count : 10
Received Port Down Count : 0
Received Generic Resp Count : 0
Received OAM Count : 0
Received Other Count : 0
Sent Syn Count : 1
Sent Synack Count : 2
Sent Rstack Count : 0
Sent Ack Count : 3
Sent Generic Resp Count : 0
Sent OAM Count : 0
Max Discovery Limit Exceed Count : 0
Result Codes: Received Sent
Invalid Request Message Count : 0 0
Specified Port(s) Down Count : 0 0
Out of Resources Count : 0 0
Request Msg Not Implemented Count : 0 0
Malformed Msg Count : 0 0
TLV Missing Count : 0 0
Invalid TLV Contents Count : 0 0
Non-Existent Port(s) Count : 0 0
<table>
<thead>
<tr>
<th>Description</th>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Port Up Count</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>Received Port Down Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Received Generic Resp Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Received Adjacency Update Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Received OAM Responses Count</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Received Other Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sent Syn Count</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Sent Synack Count</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Sent Rstack Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sent Ack Count</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Sent Generic Resp Count</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sent OAM Requests Count</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Max Discovery Limit Exceed Count</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Result Codes:</td>
<td>Received</td>
<td>Sent</td>
</tr>
<tr>
<td>Invalid Request Message Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Specified Port(s) Down Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Out of Resources Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Request Msg Not Implemented Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Malformed Msg Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TLV Missing Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Invalid TLV Contents Count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Non-Existent Port(s) Count</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**show ancp statistics**

**Syntax**

```
show ancp statistics
<ip-address ip-address>
<system-name mac-address>
```

**Release Information**

Command introduced in Junos OS Release 13.3.

**Description**

Display statistics for all ANCP neighbors (access nodes) or the specified ANCP neighbor.

**Options**

- `none`—Display statistics for all ANCP neighbors, including global statistics not show for individual neighbors.
- `ip-address ip-address`—(Optional) Display statistics for only the neighbor with the specified IP address.
- `system-name mac-address`—(Optional) Display statistics for only the neighbor with the specified MAC address.

**Required Privilege**

view

**Related Documentation**

- show ancp cos on page 1681
- show ancp neighbor on page 1686
- show ancp subscriber on page 1699

**List of Sample Output**

- show ancp statistics on page 1696
- show ancp statistics ip-address on page 1697
- show ancp statistics system-name on page 1697

**Output Fields**

Table 56 on page 1694 lists the output fields for the `show ancp statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 56: show ancp statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of neighbors</td>
<td>Total count of ANCP neighbors.</td>
</tr>
<tr>
<td>Number of subscribers</td>
<td>Total count of ANCP subscribers.</td>
</tr>
<tr>
<td>Accept Count</td>
<td>Number of neighbor TCP/IP sessions accepted on listener socket.</td>
</tr>
</tbody>
</table>
Table 56: show ancp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Fail Count</td>
<td>Number of neighbor TCP/IP sessions that failed due to one of the following causes: session already exists, maximum number of ANCP connections exceeded, creation of session or neighbor failed, or protocol start failed.</td>
</tr>
<tr>
<td>No Config Accept Deny Count</td>
<td>Number of neighbor TCP/IP sessions that failed because the neighbor was not configured.</td>
</tr>
<tr>
<td>Received Syn Count</td>
<td>Number of synchronization messages received from neighbors to maintain adjacencies.</td>
</tr>
<tr>
<td>Received Synack Count</td>
<td>Number of synchronization acknowledgment messages received from neighbors in response to the node's synchronization messages.</td>
</tr>
<tr>
<td>Received Rstack Count</td>
<td>Number of messages received from neighbors indicating that the link to the neighbor needs to be reset.</td>
</tr>
<tr>
<td>Received Ack Count</td>
<td>Number of acknowledgment messages periodically received from neighbors after an adjacency has been established.</td>
</tr>
<tr>
<td>Received Port Up Count</td>
<td>Number of status messages received from neighbors indicating that a port has transitioned to the up state.</td>
</tr>
<tr>
<td>Received Port Down Count</td>
<td>Number of status messages received from neighbors indicating that a port has transitioned to the down state.</td>
</tr>
<tr>
<td>Received Generic Resp Count</td>
<td>Number of generic response messages received from neighbors.</td>
</tr>
<tr>
<td>Received Adjacency Update Count</td>
<td>Number of adjacency update messages received from neighbors.</td>
</tr>
<tr>
<td>Received OAM Count</td>
<td>Number of OAM responses received from neighbors in reply to request commands.</td>
</tr>
<tr>
<td>Received Other Count</td>
<td>Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.</td>
</tr>
<tr>
<td>Sent Syn Count</td>
<td>Number of synchronization messages sent to neighbors to maintain adjacencies.</td>
</tr>
<tr>
<td>Sent Synack Count</td>
<td>Number of synchronization acknowledgment messages sent to neighbors in response to the their synchronization messages.</td>
</tr>
<tr>
<td>Sent Rstack Count</td>
<td>Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.</td>
</tr>
<tr>
<td>Sent Ack Count</td>
<td>Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.</td>
</tr>
<tr>
<td>Sent Generic Resp Count</td>
<td>Number of generic response messages sent to neighbors.</td>
</tr>
</tbody>
</table>
### Table 56: show ancp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent OAM Count</td>
<td>Number of OAM request commands sent to neighbors.</td>
</tr>
</tbody>
</table>

#### Result Codes

Number of generic response messages sent to neighbors that include each of the following result codes:

- **Invalid Request Message Count**—A properly formed request messages violated the protocol because of timing (such as a race condition) or direction of transmission.
- **Specified Port(s) Down Count**—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application.
- **Out of Resources Count**—the ANCP agent is out of resources, probably not related to the access lines. This result code is sent only by an access node.
- **Request Msg Not Implemented Count**—
- **Malformed Msg Count**—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection.
- **TLV Missing Count**—One or more mandatory TLVs was missing from a request.
- **Invalid TLV Contents Count**—The contents of one or more TLVs in the request do not match its required specification.
- **Non-Existent Port(s) Count**—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA.

#### Sample Output

```plaintext
show ancp statistics

user@host> show ancp statistics

Statistics
  Number of neighbors : 4
  Number of subscribers : 6
  Accept Count : 0
  Accept Fail Count : 0
  No Config Accept Deny Count : 0
  Received Syn Count : 2
  Received Synack Count : 1
  Received Rstack Count : 0
  Received Ack Count : 8
  Received Port Up Count : 7
  Received Port Down Count : 0
  Received Generic Resp Count : 0
  Received Adjacency Update Count : 0
  Received OAM Count : 0
  Received Other Count : 0
  Sent Syn Count : 1
  Sent Synack Count : 1
  Sent Rstack Count : 0
  Sent Ack Count : 17
  Sent Generic Resp Count : 0
  Sent OAM Count : 4

Result Codes: Received  Sent
  Invalid Request Message Count : 0  0
```

Copyright ©2019, Juniper Networks, Inc.
show ancp statistics ip-address

show ancp statistics ip-address 203.0.113.1

Statistics

<table>
<thead>
<tr>
<th>Received Syn Count</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Synack Count</td>
<td>1</td>
</tr>
<tr>
<td>Received Rstack Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Ack Count</td>
<td>8</td>
</tr>
<tr>
<td>Received Port Up Count</td>
<td>7</td>
</tr>
<tr>
<td>Received Port Down Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Generic Resp Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Adjacency Update Count</td>
<td>0</td>
</tr>
<tr>
<td>Received OAM Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Other Count</td>
<td>0</td>
</tr>
<tr>
<td>Sent Syn Count</td>
<td>1</td>
</tr>
<tr>
<td>Sent Synack Count</td>
<td>1</td>
</tr>
<tr>
<td>Sent Rstack Count</td>
<td>0</td>
</tr>
<tr>
<td>Sent Ack Count</td>
<td>17</td>
</tr>
<tr>
<td>Sent Generic Resp Count</td>
<td>0</td>
</tr>
<tr>
<td>Sent OAM Count</td>
<td>4</td>
</tr>
</tbody>
</table>

Result Codes:

| Invalid Request Message Count | Received | 0 |
| Specified Port(s) Down Count | 0 |
| Out of Resources Count | 0 |
| Request Msg Not Implemented Count | 0 |
| Malformed Msg Count | 0 |
| TLV Missing Count | 0 |
| Invalid TLV Contents Count | 0 |
| Non-Existent Port(s) Count | 0 |

show ancp statistics system-name

show ancp statistics system-name 00:00:5E:00:53:02

Statistics

<table>
<thead>
<tr>
<th>Received Syn Count</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Synack Count</td>
<td>1</td>
</tr>
<tr>
<td>Received Rstack Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Ack Count</td>
<td>8</td>
</tr>
<tr>
<td>Received Port Up Count</td>
<td>7</td>
</tr>
<tr>
<td>Received Port Down Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Generic Resp Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Adjacency Update Count</td>
<td>0</td>
</tr>
<tr>
<td>Received OAM Count</td>
<td>0</td>
</tr>
<tr>
<td>Received Other Count</td>
<td>0</td>
</tr>
<tr>
<td>Sent Syn Count</td>
<td>1</td>
</tr>
<tr>
<td>Sent Synack Count</td>
<td>1</td>
</tr>
<tr>
<td>Sent Rstack Count</td>
<td>0</td>
</tr>
<tr>
<td>Result Code</td>
<td>Received</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Invalid Request Message Count</td>
<td>0</td>
</tr>
<tr>
<td>Specified Port(s) Down Count</td>
<td>0</td>
</tr>
<tr>
<td>Out of Resources Count</td>
<td>0</td>
</tr>
<tr>
<td>Request Msg Not Implemented Count</td>
<td>0</td>
</tr>
<tr>
<td>Malformed Msg Count</td>
<td>0</td>
</tr>
<tr>
<td>TLV Missing Count</td>
<td>0</td>
</tr>
<tr>
<td>Invalid TLV Contents Count</td>
<td>0</td>
</tr>
<tr>
<td>Non-Existent Port(s) Count</td>
<td>0</td>
</tr>
</tbody>
</table>
show ancp subscriber

Syntax

show ancp subscriber
<brief | detail>
<access-aggregation-circuit-id circuit-identifier>
<identifier identifier>
<ip-address ip-address>
<system-name mac-address>

Release Information

Command introduced in Junos OS Release 9.4.
neighbor option replaced with ip-address in Junos OS Release 16.1.
system-name option introduced in Junos OS Release 16.1.
access-aggregation-circuit-id option introduced in Junos OS Release 18.4R1.

Description

Display information about active subscribers regardless of the subscriber's operational state, for all subscribers (local access loops), the subscriber associated with the access line specified by an ACI, or the subscriber associated with the specified ANCP neighbor (access node).

After an ancpd restart, this command displays orphaned entries (marked with an o) for subscriber sessions that were established before the restart but which have not yet been reestablished. As sessions are reestablished, the number of orphaned entries displayed by the command decreases. The number reaches zero when all sessions are reestablished or when the orphaned-interface timer expires.

Options

none—Display information about all subscribers.
brief | detail—(Optional) Display the specified level of detail.
access-aggregation-circuit-id circuit-identifier—(Optional) Display information about ANCP subscribers whose Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x0003) matches the specified value.

A circuit-identifier that begins with the # character indicates a backhaul line identifier. You can specify a wildcard (*) anywhere in the string.

identifier identifier—(Optional) Display information about the subscriber associated with the access line (ACI) specified by the access identifier.
ip-address ip-address—(Optional) Display information about the subscribers connected to the access node specified by the IP address.

system-name mac-address—(Optional) Display information about the subscribers connected to the access node specified by the MAC address.

Required Privilege

view
Related Documentation

- clear ancp subscriber on page 1675
- show ancp cos on page 1681
- show ancp neighbor on page 1686
- show ancp statistics on page 1694

List of Sample Output

- show ancp subscriber on page 1703
- show ancp subscriber (After ancpd Restart) on page 1703
- show ancp subscriber brief on page 1703
- show ancp subscriber detail on page 1703
- show ancp subscriber access-aggregation-circuit-id detail on page 1704
- show ancp subscriber identifier identifier-string detail on page 1705

Output Fields

Table 57 on page 1700 lists the output fields for the **show ancp subscriber** command. Output fields are listed in the approximate order in which they appear.

**Table 57: show ancp subscriber Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loop Identifier</td>
<td>Access loop identifier as sent by the access node and configured to map the subscriber to an interface.</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An o indicates that the entry is for an orphaned interface and represents a previously established subscriber session that has not been reestablished after an ancpd restart.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The number of orphaned entries decreases as the ANCP neighbors reestablish adjacencies and the protocol subscriber sessions are reestablished. The command output indicates this by removing the o marker.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eventually the number of orphaned entries reaches zero, because either all the adjacencies and subscriber sessions have been reestablished or any remaining orphaned entries are removed when the orphaned-interface timer expires.</td>
<td></td>
</tr>
<tr>
<td>DSL Line State</td>
<td>State of the DSL line: Idle, Showtime, or Silent.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Access Type</td>
<td>Type of access line employed by the access node: ADSL1, ADSL2, ADSL2+, VDSL1, VDSL2, SDSL, G.fast, VDSL2 Annex Q, SDSL bonded, VDSL2 bonded, G.fast bonded VDSL2 Annex Q bonded or OTHER.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface set or logical interface.</td>
<td>brief detail none</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>Rate Kbps</td>
<td>Actual downstream data rate for this local loop.</td>
<td>brief none</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address of ANCP neighbor (access node).</td>
<td>brief none</td>
</tr>
<tr>
<td>Access Loop Circuit Identifier</td>
<td>Access loop circuit identifier as sent by the access node and configured to map the subscriber to an interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</td>
<td></td>
</tr>
<tr>
<td>Neighbor IPAddress</td>
<td>IP address of the ANCP neighbor (access node).</td>
<td>detail</td>
</tr>
<tr>
<td>Aggregate Circuit Identifier</td>
<td>ASCII identifier for the subscriber access loop; value of the Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x0003).</td>
<td>detail</td>
</tr>
<tr>
<td>Aggregate Circuit Identifier Binary</td>
<td>Binary identifier for the VLAN circuit ID.</td>
<td>detail</td>
</tr>
<tr>
<td>Tech Type</td>
<td>Type of technology employed by the subscriber. Currently Junos OS supports DSL technology type only.</td>
<td>detail</td>
</tr>
<tr>
<td>DSL Line Data Link</td>
<td>Data link protocol employed on the access loop: AAL5 or Ethernet.</td>
<td>detail</td>
</tr>
<tr>
<td>DSL Line Encapsulation</td>
<td>Encapsulation type on the access loop, for Ethernet only:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 0—NA, type not conveyed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1—Untagged Ethernet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Single-tagged Ethernet</td>
<td></td>
</tr>
<tr>
<td>DSL Line Encapsulation Payload</td>
<td>Payload carried across the access loop:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 0—NA, type not conveyed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1—PPPoA LLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—PPPoA null</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—IPoA LLC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4—IPoA null</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5—Ethernet over AAL5 LLC with FCS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 6—Ethernet over AAL5 LLC without FCS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 7—Ethernet over AAL5 null with FCS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8—Ethernet over AAL5 null without FCS</td>
<td></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>Interface Type</td>
<td>Type of interface employed for subscriber traffic: ifl for a single VLAN or interface-set for a configured group of VLANs.</td>
<td>detail</td>
</tr>
<tr>
<td>Actual Net Data Upstream</td>
<td>Actual upstream data rate for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Actual Net Data Downstream</td>
<td>Actual downstream data rate for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Minimum Net Data Upstream</td>
<td>Minimum upstream data rate desired by the operator for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Minimum Net Data Downstream</td>
<td>Minimum downstream data rate desired by the operator for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum Net Data Upstream</td>
<td>Maximum upstream data rate desired by the operator for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum Net Data Downstream</td>
<td>Maximum downstream data rate desired by the operator for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Attainable Net Data Upstream</td>
<td>Maximum attainable upstream data rate for this local loop, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Attainable Net Data Downstream</td>
<td>Maximum attainable downstream data rate for this local loop.</td>
<td>detail</td>
</tr>
<tr>
<td>Minimum Low Power Data Upstream</td>
<td>Minimum downstream data rate desired by the operator for this local loop in low power state, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Minimum Low Power Data Downstream</td>
<td>Minimum upstream data rate desired by the operator for this local loop in low power state, in Kbps.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum Interleave Delay Downstream</td>
<td>Maximum interleaving delay for downstream data, in milliseconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum Interleave Delay Upstream</td>
<td>Maximum interleaving delay for upstream data, in milliseconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Actual Interleave Delay Downstream</td>
<td>Actual interleaving delay for downstream data, in milliseconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Actual Interleave Delay Upstream</td>
<td>Actual interleaving delay for upstream data, in milliseconds.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Sample Output

show ancp subscriber

```
user@host> show ancp subscriber

<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>DSL Line</th>
<th>Tech Type</th>
<th>Access Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>circuit 101</strong></td>
<td>Idle</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>circuit 102</strong></td>
<td>Idle</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>circuit 301</td>
<td>Showtime</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>circuit 302</td>
<td>Showtime</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

show ancp subscriber (After ancpd Restart)

```
user@host> show ancp subscriber

<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>DSL Line</th>
<th>Tech Type</th>
<th>Access Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>o circuit 201</td>
<td>Showtime</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.102</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o circuit 202</td>
<td>Showtime</td>
<td>DSL</td>
<td>ADSL1</td>
<td>----</td>
</tr>
<tr>
<td>203.0.113.112</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

show ancp subscriber brief

```
user@host> show ancp subscriber brief

<table>
<thead>
<tr>
<th>Loop Identifier</th>
<th>Type</th>
<th>Interface</th>
<th>Rate</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-1-10</td>
<td>VDSL2</td>
<td>set-ge-10410</td>
<td>64</td>
<td>203.0.113.102</td>
</tr>
<tr>
<td>port-1-11</td>
<td>VDSL2</td>
<td>set-ge-10411</td>
<td>64</td>
<td>203.0.113.111</td>
</tr>
<tr>
<td>port-2-10</td>
<td>VDSL2</td>
<td>ge-1/0/4.12</td>
<td>64</td>
<td>203.0.113.112</td>
</tr>
<tr>
<td>port-2-11</td>
<td>VDSL2</td>
<td>ge-1/0/4.13</td>
<td>64</td>
<td>203.0.113.113</td>
</tr>
</tbody>
</table>
```

show ancp subscriber detail

```
user@host> show ancp subscriber detail

Subscriber Information
* Access Loop Circuit Identifier : circuit 101
  Neighbor IP Address : 203.0.113.13
  Aggregate Circuit Identifier Binary : 0/0
  Tech Type : DSL
  Access Type : ADSL1
  DSL Line State : Idle
  DSL Line Data Link : Data link 2
  DSL Line Encapsulation : N/A
  DSL Line Encapsulation Payload : N/A
```
show ancp subscriber access-aggregation-circuit-iddetail

* Access Loop Circuit Identifier: circuit 102
  Neighbor IP Address: 213.0.113.13
  Aggregate Circuit Identifier Binary: 0/0
  Tech Type: DSL
  Access Type: ADSL1
  DSL Line State: Idle
  DSL Line Data Link: Data link 2
  DSL Line Encapsulation: N/A
  DSL Line Encapsulation Payload: N/A
  Interface Type: N/A
  Interface: ----
  Actual Net Data Upstream: 32
  Actual Net Data Downstream: 32
  Minimum Net Data Upstream: 0
  Minimum Net Data Downstream: 0
  Maximum Net Data Upstream: 0
  Maximum Net Data Downstream: 0
  Attainable Net Data Upstream: 1024
  Attainable Net Data Downstream: 8192
  Minimum Low Power Data Downstream: 32
  Minimum Low Power Data Upstream: 32
  Maximum Interleave Delay Downstream: 20
  Maximum Interleave Delay Upstream: 20
  Actual Interleave Delay Downstream: 20
  Actual Interleave Delay Upstream: 20

show ancp subscriber access-aggregation-circuit-iddetail

* Access Loop Circuit Identifier: circuit 201
  Neighbor IP Address: 192.0.2.1
  Access Loop Remote Identifier: remote 123
  Aggregate Circuit Identifier: #TEST-DPU-C-100
  Aggregate Circuit Identifier Binary: 50
  Tech Type: DSL
  Interface Type: interface
  Interface: ge-1/0/0.3221225475
  Actual Net Data Upstream: 1024
  Actual Net Data Downstream: 2048
  Maximum Net Data Upstream: 0
  Maximum Net Data Downstream: 0
| Access Loop Circuit Identifier : circuit 202 |
|-----------------------------|------------------|
| Neighbor IP Address        : 192.0.2.1 |
| Access Loop Remote Identifier : remote 185 |
| Aggregate Circuit Identifier : #TEST-DPU-C-100 |
| Aggregate Circuit Identifier Binary : 50 |
| Tech Type: DSL |
| Interface Type: interface |
| Interface: ge-1/0/0.3221225476 |
| Actual Net Data Upstream : 1024 |
| Actual Net Data Downstream : 2048 |
| Maximum Net Data Upstream : 0 |
| Maximum Net Data Downstream : 0 |

show ancp subscriber identifier identifier-string detail

user@host> show ancp subscriber identifier port-1-11 detail

| Access Loop Identifier : port-1-11 |
|-----------------------------|------------------|
| Neighbor IP Address        : 203.0.113.112 |
| Aggregate Circuit Identifier Binary : 0/0 |
| DSL Type: DSL 0 |
| Interface Type: interface-set |
| Interface: set-ge-10411 |
| DSL Line State : Show Time |
| Actual Net Data Upstream : 64 |
| Actual Net Data Downstream : 64 |
| DSL Line Data Link : AAL5 |
| DSL Line Encapsulation : N/A |
| DSL Line Encapsulation Payload : N/A |
| Minimum Net Data Upstream : 64 |
| Minimum Net Data Downstream : 64 |
| Maximum Net Data Upstream : 64 |
| Maximum Net Data Downstream : 64 |
| Attainable Net Data Upstream : 64 |
| Attainable Net Data Downstream : 64 |
| Minimum Low Power Data Downstream : 64 |
| Minimum Low Power Data Upstream : 64 |
| Maximum Interleave Delay Downstream : 50 |
| Maximum Interleave Delay Upstream : 50 |
| Actual Interleave Delay Downstream : 50 |
| Actual Interleave Delay Upstream : 50 |
show ancp summary

Syntax
show ancp summary

Release Information

Description
Display a summary of the counts and states for all ANCP neighbors and subscribers.

Options
This command has no options.

Required Privilege
view

Related Documentation
- show ancp neighbor on page 1686
- show ancp summary neighbor on page 1708
- show ancp subscriber on page 1699
- show ancp summary subscriber on page 1710

List of Sample Output
show ancp summary on page 1707

Output Fields
Table 58 on page 1706 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 58: show ancp summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.</td>
</tr>
<tr>
<td>Establishing</td>
<td>Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.</td>
</tr>
<tr>
<td>Established</td>
<td>Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.</td>
</tr>
<tr>
<td>Not Estabished</td>
<td>Number of ANCP neighbors in the Not Estabished state; that is, that have lost a previously established adjacency and are ready to begin negotiations.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of ANCP neighbors; sum of neighbors in the Configured, Establishing, Established, and Not Estabished states.</td>
</tr>
<tr>
<td>Showtime</td>
<td>Number of DSL lines in Showtime state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Number of DSL lines in idle state.</td>
</tr>
</tbody>
</table>
Table 58: show ancp summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent</td>
<td>Number of DSL lines in Silent state.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Number of DSL lines where the state is not Showtime, Idle, or Silent.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime, Idle, Silent, and Unknown states.</td>
</tr>
</tbody>
</table>

Sample Output

show ancp summary

user@host> show ancp summary

Neighbors Summary:

<table>
<thead>
<tr>
<th></th>
<th>Configured</th>
<th>Establishing</th>
<th>Established</th>
<th>Not Established</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>22</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>24</td>
</tr>
</tbody>
</table>

Subscribers Summary:

<table>
<thead>
<tr>
<th></th>
<th>Showtime</th>
<th>Idle</th>
<th>Silent</th>
<th>Unknown</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>
show ancp summary neighbor

Syntax

show ancp summary neighbor
<ip-address ip-address | system-name mac-address>

Release Information


Description

Display a summary of the counts and states for all ANCP neighbors and of the neighbor’s subscribers when you specify a particular neighbor.

Options

ip-address ip-address—(Optional) IP address of the ANCP neighbor (access node).

system-name mac-address—(Optional) MAC address of the ANCP neighbor (access node).

Required Privilege Level

view

Related Documentation

- show ancp summary on page 1706
- show ancp subscriber on page 1699
- show ancp summary subscriber on page 1710

List of Sample Output

show ancp summary neighbor on page 1709
show ancp summary neighbor (IP Address) on page 1709
show ancp summary neighbor (MAC Address) on page 1709

Output Fields

Table 59 on page 1708 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 59: show ancp summary neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.</td>
</tr>
<tr>
<td>Establishing</td>
<td>Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.</td>
</tr>
<tr>
<td>Established</td>
<td>Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.</td>
</tr>
<tr>
<td>NotEstablished</td>
<td>Number of ANCP neighbors in the Not Established state; that is, that have lost a previously established adjacency and are ready to begin negotiations.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of ANCP neighbors; sum of neighbors in the Configured, Establishing, Established, and NotEstablished states.</td>
</tr>
</tbody>
</table>
### Table 59: show ancp summary neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Showtime</td>
<td>Number of DSL lines for the neighbor in Showtime state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Number of DSL lines for the neighbor in Idle state.</td>
</tr>
<tr>
<td>Silent</td>
<td>Number of DSL lines for the neighbor in Silent state.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Number of DSL lines for the neighbor where the state is not Showtime, Idle, or Silent.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime, Idle, Silent, and Unknown states.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ancp summary neighbor**

```
user@host> show ancp summary neighbor

Neighbors Summary:
Configured  Establishing  Established  Not Established  Total
----------  ------------  -----------  ---------------  ----------
22             0            2                0          24
```

**show ancp summary neighbor (IP Address)**

```
user@host> show ancp summary neighbor ip-address 192.168.10.1

Neighbor Summary:192.168.10.1 status Established

Subscribers Summary:
Show Time  Idle  Silent  Unknown  Total
----------  ------  -------  --------  --------
6          0      0       0        6
```

**show ancp summary neighbor (MAC Address)**

```
user@host> show ancp summary neighbor system-name 00:00:5E:00:53:02

Neighbor Summary:00:00:5E:00:53:02 status Established

Subscribers Summary:
Show Time  Idle  Silent  Unknown  Total
----------  ------  -------  --------  --------
5          1      2       0        8
```
**show ancp summary subscriber**

**Syntax**

```
show ancp summary subscriber
```

**Release Information**


**Description**

Display a summary of the counts and states for all ANCP subscribers.

**Options**

This command has no options.

**Required Privilege Level**

view

**Related Documentation**

- show ancp summary on page 1706
- show ancp neighbor on page 1686
- show ancp summary neighbor on page 1708

**List of Sample Output**

show ancp summary subscriber on page 1710

**Output Fields**

Table 60 on page 1710 lists the output fields for the `show ancp summary subscriber` 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>Showtime</td>
<td>Number of DSL lines in Showtime state.</td>
</tr>
<tr>
<td>Idle</td>
<td>Number of DSL lines in Idle state.</td>
</tr>
<tr>
<td>Silent</td>
<td>Number of DSL lines in Silent state.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Number of DSL lines where the state is not Showtime, Idle, or Silent.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime, Idle, Silent, and Unknown states.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show ancp summary subscriber
```

```
user@host> show ancp summary subscriber

Subscribers Summary:
Show Time  Idle  Silent  Unknown  Total
```
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>
BFD Operational Commands

- clear bfd adaptation
- clear bfd session
- show bfd session
### clear bfd adaptation

**Syntax**

```
clear bfd adaptation
<string>
<all>
<address session-address>
<discriminator discr-number>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Clear adaptation for Bidirectional Forwarding Detection (BFD) sessions. BFD is a simple hello mechanism that detects failures in a network. Configured BFD interval timers can change, adapting to network situations. Use this command to return BFD interval timers to their configured values.

The `clear bfd adaptation` command is hitless, meaning that the command does not affect traffic flow on the routing device.

**Options**

- **all**—Clear adaptation for all BFD sessions.
- **address session-address**—(Optional) Clear adaptation for all BFD sessions matching the specified address.
- **discriminator discr-number**—(Optional) Clear adaptation for the local BFD session matching the specified discriminator.

**Additional Information**

For more information, see the description of the `bfd-liveness-detection` configuration statement in the *Junos Routing Protocols Configuration Guide*.

**Required Privilege Level**

`clear`

**Related Documentation**

- show bfd session on page 1717

**List of Sample Output**

- clear bfd adaptation on page 1714

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear bfd adaptation
```

```
user@host> clear bfd adaptation
```
clear bfd session

List of Syntax

Syntax

```
clear bfd session
<all>
<address session-address>
<discriminator discr-number>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and QFX Series)

```
clear bfd session
<all>
<address session-address>
<discriminator discr-number>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Drop one or more Bidirectional Forwarding Detection (BFD) sessions.

Options

- `all`—Drop all BFD sessions.
- `address session-address`—(Optional) Drop all BFD sessions matching the specified address.
- `discriminator discr-number`—(Optional) Drop the local BFD session matching the specified discriminator.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

`clear`

Related Documentation

- `show bfd session` on page 1717

List of Sample Output

- `clear bfd session all` on page 1715

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear bfd session all
user@host> clear bfd session all
```
**show bfd session**

**List of Syntax**  
Syntax on page 1717  
Syntax (EX Series Switch and QFX Series) on page 1717

**Syntax**
```
show bfd session
  <brief | detail | extensive | summary>
  <address address>
  <client rsvp-oam (brief | detail | extensive | summary) | vpls-oam (brief | detail | extensive |
  instance instance-name | summary)>
  <discriminator discriminator>
  <logical-system (all | logical-system-name)>
  <prefix address>
  <subscriber (address destination-address | discriminator discriminator | extensive)>
```

**Syntax (EX Series Switch and QFX Series)**
```
show bfd session
  <brief | detail | extensive | summary>
  <address address>
  <client rsvp-oam (brief | detail | extensive | summary) | vpls-oam (brief | detail | extensive |
  instance instance-name | summary)>
  <discriminator discriminator>
  <prefix address>
```

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Options **discriminator** and **address** introduced in Junos OS Release 8.2.  
Option **prefix** introduced in Junos OS Release 9.0.  
Command introduced in Junos OS Release 12.1 for the QFX Series.  
Option **client** introduced in Junos OS Release 12.3R3.  
Option **subscriber** introduced in Junos OS Release 15.1 for the MX Series.

**Description**  
Display information about active Bidirectional Forwarding Detection (BFD) sessions.

**Options**
- **none**—(Same as **brief**) Display information about active BFD sessions.
- **brief** | **detail** | **extensive** | **summary**—(Optional) Display the specified level of output.
- **address address**—(Optional) Display information about the BFD session for the specified neighbor address.
- **client rsvp-oam**
  - (brief | detail | extensive | summary)
  - vpls-oam
    - (brief | detail | extensive | instance instance-name | summary)—(Optional) Display information about RSVP-OAM or VPLS-OAM BFD sessions in the specified level of output. For VPLS-OAM, display the specified level of output or display information about all of the BFD sessions for the specified VPLS routing instance.
**discriminator discriminator**—(Optional) Display information about the BFD session using the specified local discriminator.

**logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**<subscriber (address destination-address | discriminator discriminator | extensive)>**—(Optional) Display information about all BFD sessions for subscribers, or for a single BFD subscriber session with a particular destination address, or with a particular denominator.

**Required Privilege Level**

`view`

**Related Documentation**

- clear bfd session on page 1715
- Understanding BFD for Static Routes for Faster Network Failure Detection
- Example: Configuring BFD for Static Routes for Faster Network Failure Detection
- Understanding BFD for OSPF
- Example: Configuring BFD for OSPF
- Understanding BFD for BGP
- Example: Configuring BFD on Internal BGP Peer Sessions
- Understanding Bidirectional Forwarding Detection Authentication for PIM
- Configuring BFD for PIM
- Understanding BFD for IS-IS

**List of Sample Output**

- show bfd session on page 1722
- show bfd session brief on page 1723
- show bfd session detail on page 1723
- show bfd session detail (with Authentication) on page 1723
- show bfd session address extensive on page 1723
- show bfd session client rsvp-oam on page 1724
- show bfd session client vpls-oam summary on page 1724
- show bfd session client vpls-oam instance instance-name on page 1724
- show bfd session extensive on page 1724
- show bfd session extensive (with Authentication) on page 1725
- show bfd session summary on page 1726
- show bfd session subscriber on page 1726
- show bfd session subscriber address on page 1726
- show bfd session subscriber extensive on page 1726
- show bfd session subscriber discriminator extensive on page 1727

**Output Fields**

Table 61 on page 1719 describes the output fields for the `show bfd session` command. Output fields are listed in the approximate order in which they appear.
### Table 61: show bfd session Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Address on which the BFD session is active.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>State</td>
<td>State of the BFD session: <strong>Up</strong>, <strong>Down</strong>, <strong>Init</strong> (initializing), or <strong>Failing</strong>.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the BFD session is active.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Detect Time</td>
<td>Negotiated time interval, in seconds, used to detect BFD control packets.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Transmit Interval</td>
<td>Time interval, in seconds, used by the transmitting system to send BFD control packets.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Multiplier</td>
<td>Negotiated multiplier by which the time interval is multiplied to determine the detection time for the transmitting system.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Session up time</td>
<td>How long a BFD session has been established.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Client</td>
<td>Protocol or process for which the BFD session is active: <strong>ISIS</strong>, <strong>OSPF</strong>, <strong>DHCP</strong>, <strong>Static</strong>, or <strong>VGD</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>TX interval</td>
<td>Time interval, in seconds, used by the host system to transmit BFD control packets.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>RX interval</td>
<td>Time interval, in seconds, used by the host system to receive BFD control packets.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Authenticate</td>
<td>Indicates that BFD authentication is configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>keychain</td>
<td>Name of the security authentication keychain being used by a specific client. BFD authentication information for a client is provided in a single line and includes the keychain, algo, and mode parameters. Multiple clients can be configured on a BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td>algo</td>
<td>BFD authentication algorithm being used for a specific client: <strong>keyed-md5</strong>, <strong>keyed-sha-1</strong>, <strong>meticulous-keyed-md5</strong>, <strong>meticulous-keyed-sha-1</strong>, or <strong>simple-password</strong>. BFD authentication information for a client is provided in a single line and includes the keychain, algo, and mode parameters. Multiple clients can be configured on a BFD session.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 61: `show bfd session` 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>mode</strong></td>
<td>Level of BFD authentication enforcement being used by a specific client: <strong>strict</strong> or <strong>loose</strong>. Strict enforcement indicates that authentication is configured at both ends of the session (the default). Loose enforcement indicates that one end of the session might not be authenticated. BFD authentication information for a client is provided in a single line and includes the <strong>keychain</strong>, <strong>algo</strong>, and <strong>mode</strong> parameters. Multiple clients can be configured on a BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Local diagnostic</strong></td>
<td>Local diagnostic information about failing BFD sessions. Following are the expected values for Local Diagnostic output field:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No diagnostic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CtlExpire</strong>—Control detection time expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>EchoExpire</strong>—Echo detection time expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>NbrSignal</strong>—Neighbor signalled session down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FwdPlaneReset</strong>—Forwarding plane reset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PathDown</strong>—Path down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ConcatPathDown</strong>—Concatenated path down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AdminDown</strong>—Administratively down</td>
<td></td>
</tr>
<tr>
<td><strong>Remote diagnostic</strong></td>
<td>Remote diagnostic information about failing BFD sessions. Following are the expected values for Remote Diagnostic output field:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No diagnostic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CtlExpire</strong>—Control detection time expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>EchoExpire</strong>—Echo detection time expired</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>NbrSignal</strong>—Neighbor signalled session down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FwdPlaneReset</strong>—Forwarding plane reset</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>PathDown</strong>—Path down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ConcatPathDown</strong>—Concatenated path down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>AdminDown</strong>—Administratively down</td>
<td></td>
</tr>
<tr>
<td><strong>Remote state</strong></td>
<td>Reports whether the remote system’s BFD packets have been received and whether the remote system is receiving transmitted control packets.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>BFD version: 0 or 1.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Replicated</strong></td>
<td>The <strong>replicated</strong> flag appears when nonstop routing or graceful Routing Engine switchover is configured and the BFD session has been replicated to the backup Routing Engine.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Min async interval</strong></td>
<td>Minimum amount of time, in seconds, between asynchronous control packet transmissions across the BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Min slow interval</strong></td>
<td>Minimum amount of time, in seconds, between synchronous control packet transmissions across the BFD session.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 61: show bfd session Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive async TX interval</td>
<td>Transmission interval being used because of adaptation.</td>
<td>extensive</td>
</tr>
<tr>
<td>RX interval</td>
<td>Minimum required receive interval.</td>
<td>extensive</td>
</tr>
<tr>
<td>Local min TX interval</td>
<td>Minimum amount of time, in seconds, between control packet transmissions on the local system.</td>
<td>extensive</td>
</tr>
<tr>
<td>Local min RX interval</td>
<td>Minimum amount of time, in seconds, between control packet detections on the local system.</td>
<td>extensive</td>
</tr>
<tr>
<td>Remote min TX interval</td>
<td>Minimum amount of time, in seconds, between control packet transmissions on the remote system.</td>
<td>extensive</td>
</tr>
<tr>
<td>Remote min RX interval</td>
<td>Minimum amount of time, in seconds, between control packet detections on the remote system.</td>
<td>extensive</td>
</tr>
<tr>
<td>Threshold transmission interval</td>
<td>Threshold for notification if the transmission interval increases.</td>
<td>extensive</td>
</tr>
<tr>
<td>Threshold for detection time</td>
<td>Threshold for notification if the detection time increases.</td>
<td>extensive</td>
</tr>
<tr>
<td>Local discriminator</td>
<td>Authentication code used by the local system to identify that BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td>Remote discriminator</td>
<td>Authentication code used by the remote system to identify that BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td>Echo mode</td>
<td>Information about the state of echo transmissions on the BFD session.</td>
<td>extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>LDP FEC address associated with the BFD session.</td>
<td>All levels</td>
</tr>
<tr>
<td>Egress, Destination</td>
<td>Displays the LDP FEC destination address. This field is displayed only on a router at the egress of an LDP FEC, where the BFD session has an LDP Operation, Administration, and Maintenance (OAM) client.</td>
<td>All levels</td>
</tr>
<tr>
<td>Remote is control-plane independent</td>
<td>The BFD session on the remote peer is running on its Packet Forwarding Engine.  In this case, when the remote node undergoes a graceful restart, the local peer can help the remote peer with the graceful restart.  The following BFD sessions are not distributed to the Packet Forwarding Engine: tunnel-encapsulated sessions, and sessions over integrated routing and bridging (IRB) interfaces.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 61: show bfd session Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Summary status of BFD authentication:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• status—enabled/active indicates authentication is configured and active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• enabled/inactive indicates authentication is configured but not active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This only occurs when the remote end of the session does not support authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• keychain—Name of the security authentication keychain associated with the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• algo—BFD authentication algorithm being used: keyed-md5, keyed-sha-1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• meticulous-keyed-md5, meticulous-keyed-sha-1, or simple-password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• mode—Level of BFD authentication enforcement: strict or loose.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strict enforcement indicates authentication is configured at both ends of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>session (the default). Loose enforcement indicates that one end of the session</td>
<td></td>
</tr>
<tr>
<td></td>
<td>might not be authenticated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This information is only shown if BFD authentication is configured.</td>
<td></td>
</tr>
<tr>
<td>Session ID</td>
<td>The BFD session ID number that represents the protection using MPLS fast</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>reroute (FRR) and loop-free alternate (LFA).</td>
<td></td>
</tr>
<tr>
<td>sessions</td>
<td>Total number of active BFD sessions.</td>
<td>All levels</td>
</tr>
<tr>
<td>clients</td>
<td>Total number of clients that are hosting active BFD sessions.</td>
<td>All levels</td>
</tr>
<tr>
<td>Cumulative transmit rate</td>
<td>Total number of BFD control packets transmitted per second on all active sessions.</td>
<td>All levels</td>
</tr>
<tr>
<td>Cumulative receive rate</td>
<td>Total number of BFD control packets received per second on all active sessions.</td>
<td>All levels</td>
</tr>
<tr>
<td>Multi-hop, min-recv-TTL</td>
<td>Minimum time to live (TTL) accepted if the session is configured for multihop.</td>
<td>extensive</td>
</tr>
<tr>
<td>route table</td>
<td>Route table used if the session is configured for multihop.</td>
<td>extensive</td>
</tr>
<tr>
<td>local address</td>
<td>Local address of the source used if the session is configured for multihop.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

**Sample Output**

```bash
user@host> show bfd session
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Transmit Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.9.1.33</td>
<td>Up</td>
<td>so-7/1/0.0</td>
<td>0.600</td>
<td>0.200</td>
<td>3</td>
</tr>
<tr>
<td>10.9.1.29</td>
<td>Up</td>
<td>ge-4/0/0.0</td>
<td>0.600</td>
<td>0.200</td>
<td>3</td>
</tr>
</tbody>
</table>
```
2 sessions, 2 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps

**show bfd session brief**

The output for the `show bfd session brief` command is identical to that for the `show bfd session` command.

**show bfd session detail**

```bash
user@host> show bfd session detail
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.9.1.33</td>
<td>Up</td>
<td>so-7/1/0.0</td>
<td>0.600</td>
<td>0.200</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3
Session up time 3d 00:34:02
Local diagnostic None, remote diagnostic None
Remote state Up, version 1
Replicated

10.9.1.29    Up    ge-4/0/0.0    0.600    0.200    3

Client ISIS L2, TX interval 0.200, RX interval 0.200, multiplier 3
Session up time 3d 00:29:04, previous down time 00:00:01
Local diagnostic NbrSignal, remote diagnostic AdminDown
Remote state Up, version 1

2 sessions, 2 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps

**show bfd session detail (with Authentication)**

```bash
user@host> show bfd session detail
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.9.1.33</td>
<td>Up</td>
<td>so-7/1/0.0</td>
<td>0.600</td>
<td>0.200</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Client OSPF, TX interval 0.200, RX interval 0.200, multiplier 3, **Authenticate**
Session up time 3d 00:34:18
Local diagnostic None, remote diagnostic None
Remote state Up, version 1
Replicated

10.9.1.29    Up    ge-4/0/0.0    0.600    0.200    3

Client ISIS L2, TX interval 0.200, RX interval 0.200, multiplier 3
Session up time 3d 00:29:12, previous down time 00:00:01
Local diagnostic NbrSignal, remote diagnostic AdminDown
Remote state Up, version 1

2 sessions, 2 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps

**show bfd session address extensive**

```bash
user@host> show bfd session 10.255.245.212 extensive
```

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.212</td>
<td>Up</td>
<td></td>
<td>1.200</td>
<td>0.400</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Client Static, TX interval 0.400, RX interval 0.400, multiplier 3
Session up time 00:17:03, previous down time 00:00:14
Local diagnostic CtlExpire, remote diagnostic NbrSignal
Remote state Up, version 1
Replicated
Min async interval 0.400, min slow interval 1.000
Adaptive async tx interval 0.400, rx interval 0.400
Local min tx interval 0.400, min rx interval 0.400, multiplier 3
Remote min tx interval 0.400, min rx interval 0.400, multiplier 3
Threshold transmission interval 0.000, Threshold for detection time 0.000
Local discriminator 6, remote discriminator 16
Echo mode disabled/inactive
Multi-hop, min-recv-TTL 255, route-table 0, local-address 10.255.245.205

1 sessions, 1 clients
Cumulative transmit rate 2.5 pps, cumulative receive rate 2.5 pps

### show bfd session client rsvp-oam

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Transmit Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.223</td>
<td>Up</td>
<td></td>
<td>540.000</td>
<td>180.000</td>
<td>3</td>
</tr>
</tbody>
</table>

1 Up sessions, 0 Down sessions
1 sessions, 1 clients
Cumulative transmit rate 0.0 pps, cumulative receive rate 0.0 pps

### show bfd session client vpls-oam summary

1 Up sessions, 1 Down sessions
2 sessions, 2 clients
Cumulative transmit rate 2.0 pps, cumulative receive rate 1.0 pps

### show bfd session client vpls-oam instance instance-name

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Transmit Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>Up</td>
<td>ae9.0</td>
<td>3.000</td>
<td>1.000</td>
<td>3</td>
</tr>
</tbody>
</table>

1 Up Sessions, 0 Down Sessions
1 sessions, 1 clients
Cumulative transmit rate 1.0 pps, cumulative receive rate 1.0 pps

### show bfd session extensive

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Detect Time</th>
<th>Transmit Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.31.1.2</td>
<td>Up</td>
<td>ge-2/1/0.0</td>
<td>0.030</td>
<td>0.010</td>
<td>3</td>
</tr>
</tbody>
</table>

Client OSPF realm ospf-v2 Area 0.0.0.0, TX interval 0.010, RX interval 0.010
Session up time 00:10:13  
Local diagnostic None, remote diagnostic None  
Remote state Up, version 1  
Replicated  
Min async interval 0.010, min slow interval 1.000  
Adaptive async TX interval 0.010, RX interval 0.010  
Local min TX interval 0.010, minimum RX interval 0.010, multiplier 3  
Remote min TX interval 0.010, min RX interval 0.010, multiplier 3  
Local discriminator 12, remote discriminator 4  
Echo mode disabled/inactive  
Remote is control-plane independent  
Session ID: 0x201  
Micro-BFD Session  

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.31.2.2</td>
<td>Up</td>
<td>ge-2/1/4.0</td>
<td>0.030</td>
<td>0.010</td>
<td>3</td>
</tr>
</tbody>
</table>

Client OSPF realm ospf-v2 Area 0.0.0.0, TX interval 0.010, RX interval 0.010  
Session up time 00:10:14  
Local diagnostic None, remote diagnostic NbrSignal  
Remote state Up, version 1  
Replicated  
Min async interval 0.010, min slow interval 1.000  
Adaptive async TX interval 0.010, RX interval 0.010  
Local min TX interval 0.010, minimum RX interval 0.010, multiplier 3  
Remote min TX interval 0.010, min RX interval 0.010, multiplier 3  
Local discriminator 13, remote discriminator 5  
Echo mode disabled/inactive  
Remote is control-plane independent  
Session ID: 0x202  

2 sessions, 2 clients  
Cumulative transmit rate 200.0 pps, cumulative receive rate 200.0 pps

---

show bfd session extensive (with Authentication)

```
user@host> show bfd session extensive

Detect   Transmit

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.208.26</td>
<td>Up</td>
<td>so-1/0/0.0</td>
<td>2.400</td>
<td>0.800</td>
<td>10</td>
</tr>
</tbody>
</table>

Client Static, TX interval 0.600, RX interval 0.600, Authenticate  
keychain bfd, algo keyed-md5, mode loose  
Session up time 00:18:07  
Local diagnostic None, remote diagnostic NbrSignal  
Remote state Up, version 1  
Replicated  
Min async interval 0.600, min slow interval 1.000  
Adaptive async TX interval 0.600, RX interval 0.600  
Local min TX interval 0.600, minimum RX interval 0.600, multiplier 10  
Remote min TX interval 0.800, min RX interval 0.800, multiplier 3  
Local discriminator 2, remote discriminator 3  
Echo mode disabled/inactive  
Authentication enabled/active, keychain bfd, algo keyed-md5, mode loose
```

1 sessions, 1 clients  
Cumulative transmit rate 1.2 pps, cumulative receive rate 1.2 pps
show bfd session summary

```
user@host> show bfd session summary
2 sessions, 2 clients
Cumulative transmit rate 10.0 pps, cumulative receive rate 10.0 pps
```

show bfd session subscriber

```
user@host> show bfd session subscriber

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.2</td>
<td>Up</td>
<td>ae0.0</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
<tr>
<td>1.0.0.6</td>
<td>Up</td>
<td>ae0.1</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
<tr>
<td>1.0.0.10</td>
<td>Up</td>
<td>ae0.2</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
<tr>
<td>1.0.0.14</td>
<td>Up</td>
<td>ae0.3</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
<tr>
<td>1.0.0.18</td>
<td>Up</td>
<td>ae0.4</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
</tbody>
</table>

20 sessions, 20 clients
```

show bfd session subscriber address

```
user@host> show bfd session subscriber address 1.0.0.2

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.2</td>
<td>Up</td>
<td>ae0.0</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
</tbody>
</table>

1 sessions, 1 clients
Cumulative transmit rate 5.0 pps, cumulative receive rate 5.0 pps
```

show bfd session subscriber extensive

```
user@host> show bfd session subscriber extensive

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.2</td>
<td>Up</td>
<td>ae0.0</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
</tbody>
</table>

Client DHCP, TX interval 30.000, RX interval 30.000
Session up time 09:11:50
Local diagnostic None, remote diagnostic NbrSignal
Remote state Up, version 1
Replicated
Min async interval 30.000, min slow interval 30.000
Adaptive async TX interval 30.000, RX interval 30.000
Local min TX interval 30.000, minimum RX interval 30.000, multiplier 3
Remote min TX interval 30.000, min RX interval 30.000, multiplier 3
Local discriminator 20, remote discriminator 16
Echo mode disabled/inactive
Remote is control-plane independent
Session ID: 0x1

<table>
<thead>
<tr>
<th>Address</th>
<th>State</th>
<th>Interface</th>
<th>Time</th>
<th>Interval</th>
<th>Multiplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.6</td>
<td>Up</td>
<td>ae0.1</td>
<td>90.000</td>
<td>30.000</td>
<td>3</td>
</tr>
</tbody>
</table>

Client DHCP, TX interval 30.000, RX interval 30.000
Session up time 09:11:50
Local diagnostic None, remote diagnostic NbrSignal
Remote state Up, version 1
Replicated
Min async interval 30.000, min slow interval 30.000
Adaptive async TX interval 30.000, RX interval 30.000
Local min TX interval 30.000, minimum RX interval 30.000, multiplier 3
Remote min TX interval 30.000, min RX interval 30.000, multiplier 3
Local discriminator 21, remote discriminator 17
Echo mode disabled/inactive
Remote is control-plane independent
Session ID: 0x2

<table>
<thead>
<tr>
<th>Detect</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>State</td>
</tr>
<tr>
<td>1.0.0.2</td>
<td>Up</td>
</tr>
</tbody>
</table>

Client DHCP, TX interval 30.000, RX interval 30.000
Session up time 09:11:50
Local diagnostic None, remote diagnostic NbrSignal
Remote state Up, version 1
Replicated
Min async interval 30.000, min slow interval 30.000
Adaptive async TX interval 30.000, RX interval 30.000
Local min TX interval 30.000, minimum RX interval 30.000, multiplier 3
Remote min TX interval 30.000, min RX interval 30.000, multiplier 3
Local discriminator 20, remote discriminator 16
Echo mode disabled/inactive
Remote is control-plane independent
Session ID: 0x1

1 sessions, 1 clients
Cumulative transmit rate 5.0 pps, cumulative receive rate 5.0 pps
CHAPTER 17

BGP Operational Commands

- clear bgp damping
- clear bgp neighbor
- clear bgp table
- show bgp bmp
- show bgp group
- show bgp group traffic-statistics
- show bgp neighbor
- show bgp replication
- show bgp summary
- show policy damping
clear bgp damping

List of Syntax
Syntax on page 1730
Syntax (EX Series Switch and QFX Series) on page 1730

Syntax
clear bgp damping
<logical-system (all | logical-system-name)>
<prefix>

Syntax (EX Series Switch and QFX Series)
clear bgp damping
<prefix>

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Clear BGP route flap damping information.

Options
none—Clear all BGP route flap damping information.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

prefix—(Optional) Clear route flap damping information for only the specified destination prefix.

Required Privilege
Level
clear

Related Documentation
• show policy damping on page 1777
• show route damping on page 2299

List of Sample Output
clear bgp damping on page 1730

Output Fields
This command produces no output.

Sample Output
clear bgp damping

user@host> clear bgp damping
clear bgp neighbor

List of Syntax

Syntax on page 1731
Syntax (EX Series Switch and QFX Series) on page 1731

Syntax

```
clear bgp neighbor
  <all>
  <as as-number>
  <gracefully>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <malformed-route>
  <neighbor>
  <soft | soft-inbound>
  <soft-minimum-igp>
  <stale-routes>
```

Syntax (EX Series Switch and QFX Series)

```
clear bgp neighbor
  <all>
  <as as-number>
  <instance instance-name>
  <malformed-route>
  <neighbor>
  <soft | soft-inbound>
  <soft-minimum-igp>
```

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

- malformed-route option introduced in Junos OS Release 13.2.
- all option introduced in Junos OS Release 14.2.
- gracefully and stale-routes options introduced in Junos OS Release 15.1.

Description

Perform one of the following tasks:

- Change the state of one or more BGP neighbors to IDLE. For neighbors in the ESTABLISHED state, this command drops the TCP connection to the neighbors and then reestablishes the connection.

- (soft keyword only) Reapply export policies and send refresh updates to one or more BGP neighbors without changing their state.

- (soft-inbound keyword only) Send a route-refresh message to one or more BGP neighbors without changing their state, and reapply import policies on the received updates.

Options

- all—Change the state of all BGP neighbors to IDLE.
as as-number—(Optional) Apply this command only to neighbors in the specified autonomous system (AS).

gracefully—(Optional) Enable the BGP peer to start graceful-restart receiving-speaker mode. The receiving speaker also sends its own routes to the restarted speaker, and sends an End-of-RIB marker when it completes the update. The `clear bgp neighbor neighbor-address gracefully` command is the same as `clear bgp neighbor hard` (the default for `clear bgp neighbor`), but it does not use the new Hard Reset subcode on the Notify and Cease messages that are sent. This allows the neighbor to enter GR or LLGR helper mode, if negotiated. The session is still cleared on this router, and this router does not enter GR or LLGR helper mode.

instance instance-name—(Optional) Apply this command only to neighbors for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

malformed-route—(Optional) Remove malformed routes. If a specific neighbor is provided, Junos OS removes malformed routes for that particular neighbor. Otherwise, Junos OS removes malformed routes for all BGP neighbors. To find routes that have malformed attributes, run the `show route hidden` command, and look for routes marked with `MalformedAttr` in the AS path field.

neighbor—(Optional) IP address of a BGP peer. Apply this command only to the specified neighbor.

soft—(Optional) Reapply any export policies and send refresh updates to neighbors without clearing the state.

soft-inbound—(Optional) Send a route-refresh message to BGP neighbors and reapply import policies on the route updates received from the BGP neighbors without clearing the BGP state.

soft-minimum-igp—(Optional) Provide soft refresh of the outbound state when the interior gateway protocol (IGP) metric is reset.

stale-routes—(Optional) Any stale route currently being held for the specified neighbor because of BGP graceful restart (GR) or long-lived graceful restart (LLGR) receiver mode operations.

Required Privilege Level: clear

Related Documentation:
- `show bgp neighbor` on page 1748

List of Sample Output:
- `clear bgp neighbor` on page 1733

Output Fields:
When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear bgp neighbor

user@host> clear bgp neighbor
clear bgp table

Syntax

```
Syntax (EX Series Switch and QFX Series)
clear bgp table table-name
logical-system (all | logical-system-name)
```

Release Information

- Command introduced in Junos OS Release 9.0.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Request that BGP refresh routes in a specified routing table.

Options

- `logical-system (all | logical-system-name)` — (Optional) Perform this operation on all logical systems or on a particular logical system.
- `table-name` — Request that BGP refresh routes in the specified table.

Additional Information

In some cases, a prefix limit is associated with a routing table for a VPN instance. When this limit is exceeded (for example, because of a network misconfiguration), some routes might not be inserted in the table. Such routes need to be added to the table after the network issue is resolved. Use the `clear bgp table` command to request that BGP refresh routes in a VPN instance table.

Required Privilege Level

- `clear`

List of Sample Output

- `clear bgp table private.inet.0 on page 1734`
- `clear bgp table inet.6 logical-system all on page 1734`
- `clear bgp table private.inet.6 logical-system ls1 on page 1735`
- `clear bgp table logical-system all inet.0 on page 1735`
- `clear bgp table logical-system ls2 private.inet.0 on page 1735`

Output Fields

This command produces no output.

Sample Output

```
clear bgp table private.inet.0
user@host> clear bgp table private.inet.0

clear bgp table inet.6 logical-system all
user@host> clear bgp table inet.6 logical-system all
```
clear bgp table private.inet.6 logical-system ls1
    user@host> clear bgp table private.inet.6 logical-system ls1

clear bgp table logical-system all inet.0
    user@host> clear bgp table logical-system all inet.0

clear bgp table logical-system ls2 private.inet.0
    user@host> clear bgp table logical-system ls2 private.inet.0
show bgp bmp

Syntax   show bgp bmp

Release Information Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 13.2X51-D15 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display information about the BGP Monitoring Protocol (BMP).

Options  This command has no options.

Required Privilege view

Level

List of Sample Output show bgp bmp on page 1736

Output Fields Table 62 on page 1736 lists the output fields for the show bgp bmp command. Output fields are listed in the approximate order in which they appear.

Table 62: show bgp bmp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMP station address/port</td>
<td>IP address and port number of the monitoring station to which BGP Monitoring Protocol (BMP) statistics are sent.</td>
</tr>
<tr>
<td>BMP session state</td>
<td>Status of the BMP session: UP or DOWN.</td>
</tr>
<tr>
<td>Statistics timeout</td>
<td>Amount of time, in seconds, between transmissions of BMP data to the monitoring station.</td>
</tr>
</tbody>
</table>

Sample Output

show bgp bmp

user@host> show bgp bmp

BMP station address/port: 172.24.24.157+5454
BMP session state: DOWN
Statistics timeout: 15
show bgp group

List of Syntax  
Syntax on page 1737
Syntax (EX Series Switch and QFX Series) on page 1737

Syntax  
show bgp group
  <brief | detail | summary>
  <group-name>
  <exact-instance instance-name>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <rtf>

Syntax (EX Series Switch and QFX Series)  
show bgp group
  <brief | detail | summary>
  <group-name>
  <exact-instance instance-name>
  <instance instance-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
exact-instance option introduced in Junos OS Release 11.4.
From Junos OS release 18.4 onwards, show bgp group group-name does an exact match and displays groups with names matching exactly with that of the specified group-name.
For all Junos OS releases preceding 18.4, the implementation was performed using the prefix matches (example: if there are two groups grp1, grp2 and the CLI command show bgp group grp was issued, then both grp1, grp2 were displayed).

Description  
Display information about the configured BGP groups.

Options  none—Display group information about all BGP groups.

brief | detail | summary—(Optional) Display the specified level of output.

group-name—(Optional) Display group information for the specified group.

exact-instance instance-name—(Optional) Display information for the specified instance only.

instance instance-name—(Optional) Display information about BGP groups for all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the show bgp group instance cust1 command). The instance name can be master for the main instance, or any valid configured instance name or its prefix.
logical-system (all | logical-system-name) — (Optional) Perform this operation on all logical systems or on a particular logical system.

rtf — (Optional) Display BGP group route targeting information.

Required Privilege
Level
view

List of Sample Output
show bgp group on page 1741
show bgp group on page 1741
show bgp group brief on page 1742
show bgp group detail on page 1742
show bgp group rtf detail on page 1744
show bgp group summary on page 1744

Output Fields
Table 63 on page 1738 describes the output fields for the show bgp group command. Output fields are listed in the approximate order in which they appear.

Table 63: show bgp group Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Type or Group</td>
<td>Type of BGP group: Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td>group-index</td>
<td>Index number for the BGP peer group. The index number differentiates between groups when a single BGP group is split because of different configuration options at the group and peer levels.</td>
<td>rtf detail</td>
</tr>
<tr>
<td>AS</td>
<td>AS number of the peer. For internal BGP (IBGP), this number is the same as Local AS.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Local AS</td>
<td>AS number of the local routing device.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Name</td>
<td>Name of a specific BGP group.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Options</td>
<td>The Network Layer Reachability Information (NLRI) format used for BGP VPN multicast.</td>
<td>none none</td>
</tr>
<tr>
<td>Index</td>
<td>Unique index number of a BGP group.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Flags</td>
<td>Flags associated with the BGP group. This field is used by Juniper Networks customer support.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>BGP-Static Advertisement Policy</td>
<td>Policies configured for the BGP group with the advertise-bgp-static policy statement.</td>
<td>brief none</td>
</tr>
</tbody>
</table>
### Table 63: `show bgp group` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove-private options</td>
<td>Options associated with the <code>remove-private</code> statement.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Maximum number of seconds allowed to elapse between successive keep alive or update messages that BGP receives from a peer in the BGP group, after which the connection to the peer is closed and routing devices through that peer become unavailable.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Export</td>
<td>Export policies configured for the BGP group with the <code>export</code> statement.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Optimal Route Reflection</td>
<td>Client nodes (primary and backup) configured in the BGP group.</td>
<td>brief detail</td>
</tr>
<tr>
<td>MED tracks IGP metric update delay</td>
<td>Time, in seconds, that updates to multiple exit discriminator (MED) are delayed. Also displays the time remaining before the interval is set to expire.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic Statistics Interval</td>
<td>Time between sample periods for labeled-unicast traffic statistics, in seconds.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Total peers</td>
<td>Total number of peers in the group.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Established</td>
<td>Number of peers in the group that are in the established state.</td>
<td>All levels</td>
</tr>
<tr>
<td>Active/Received/Accepted/Damped</td>
<td>Multipurpose field that displays information about BGP peer sessions. The field's contents depend upon whether a session is established and whether it was established in the main routing device or in a routing instance.</td>
<td>summary</td>
</tr>
<tr>
<td></td>
<td>• If a peer is not established, the field shows the state of the peer session: Active, Connect, or Idle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If a BGP session is established in the main routing device, the field shows the number of active, received, accepted, and damped routes that are received from a neighbor and appear in the inet.0 (main) and inet.2 (multicast) routing tables. For example, 8/10/10/2 and 2/4/4/0 indicate the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8 active routes, 10 received routes, 10 accepted routes, and 2 damped routes from a BGP peer appear in the inet.0 routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 active routes, 4 received routes, 4 accepted routes, and no damped routes from a BGP peer appear in the inet.2 routing table.</td>
<td></td>
</tr>
<tr>
<td>ip-addresses</td>
<td>List of peers who are members of the group. The address is followed by the peer's port number.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 63: show bgp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Queue Timer</td>
<td>Number of seconds until queued routes are sent. If this time has already elapsed, this field displays the number of seconds by which the updates are delayed.</td>
<td>detail</td>
</tr>
<tr>
<td>Route Queue</td>
<td>Number of prefixes that are queued up for sending to the peers in the group.</td>
<td>detail</td>
</tr>
<tr>
<td>inet.number</td>
<td>Number of active, received, accepted, and damped routes in the routing table. For example, <em>inet.0:7/10/9/0</em> indicates the following:</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• 7 active routes, 10 received routes, 9 accepted routes, and no damped routes from a BGP peer appear in the <em>inet.0</em> routing table.</td>
<td></td>
</tr>
<tr>
<td>Table inet.number</td>
<td>Information about the routing table.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Received prefixes</strong>—Total number of prefixes from the peer, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active prefixes</strong>—Number of prefixes received from the peer that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suppressed due to damping</strong>—Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Advertised prefixes</strong>—Number of prefixes advertised to a peer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Received external prefixes</strong>—Total number of prefixes from the external BGP (EBGP) peers, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active external prefixes</strong>—Number of prefixes received from the EBGP peers that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Externalss suppressed</strong>—Number of routes received from EBGP peers currently inactive because of damping or other reasons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Received internal prefixes</strong>—Total number of prefixes from the IBGP peers, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active internal prefixes</strong>—Number of prefixes received from the IBGP peers that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Internals suppressed</strong>—Number of routes received from IBGP peers currently inactive because of damping or other reasons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RIB State</strong>—Status of the graceful restart process for this routing table: <strong>BGP restart is complete</strong>, <strong>BGP restart in progress</strong>, <strong>VPN restart in progress</strong>, or <strong>VPN restart is complete</strong>.</td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>Total number of groups.</td>
<td>All levels</td>
</tr>
<tr>
<td>Peers</td>
<td>Total number of peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>External</td>
<td>Total number of external peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Internal</td>
<td>Total number of internal peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Down peers</td>
<td>Total number of unavailable peers.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 63: show bgp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flaps</td>
<td>Total number of flaps that occurred.</td>
<td>All levels</td>
</tr>
<tr>
<td>Table</td>
<td>Name of a routing table.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Tot Paths</td>
<td>Total number of routes.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Act Paths</td>
<td>Number of active routes.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td>brief, none</td>
</tr>
<tr>
<td>History</td>
<td>Number of withdrawn routes stored locally to keep track of damping history.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Damp State</td>
<td>Number of active routes with a figure of merit greater than zero, but lower than the threshold at which suppression occurs.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Pending</td>
<td>Routes being processed by the BGP import policy.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Group</td>
<td>Group the peer belongs to in the BGP configuration.</td>
<td>detail</td>
</tr>
<tr>
<td>Receive mask</td>
<td>Mask of the received target included in the advertised route.</td>
<td>detail</td>
</tr>
<tr>
<td>Entries</td>
<td>Number of route entries received.</td>
<td>detail</td>
</tr>
<tr>
<td>Target</td>
<td>Route target that is to be passed by route-target filtering. If a route advertised from the provider edge (PE) routing device matches an entry in the route-target filter, the route is passed to the peer.</td>
<td>detail</td>
</tr>
<tr>
<td>Mask</td>
<td>Mask which specifies that the peer receive routes with the given route target.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show bgp group

```
user@host> show bgp group
Group Type: Internal AS: 200 Local AS: 200
Name: ibgp Index: 0 Flags: <>
Options: Preference LocalAddress Cluster AddressFamily Refresh
```

show bgp group

```
user@host> show bgp group
```
show bgp group brief

Groups: 2  Peers: 2  External: 0  Internal: 2  Down peers: 1  Flaps: 0
Table Tot Paths Act Paths Suppressed History Damp State Pending
inet.0 0 0 0 0 0 0
bgp.l3vpn.0 0 0 0 0 0 0
bgp.rtarget.0 2 0 0 0 0 0

show bgp group detail

Group Type: Internal  AS: 1  Local AS: 1
Name: ibgp  Index: 0  Flags: <Export Eval>
Holdtime: 0
Optimal Route Reflection: igp-primary 1.1.1.1, igp-backup 1.1.2.1
Total peers: 3 Established: 0
22.0.0.2
22.0.0.8
22.0.0.5

Groups: 1 Peers: 3 External: 0 Internal: 3 Down peers: 3 Flaps: 3

Table bgp.l3vpn.0
Received prefixes: 0
Accepted prefixes: 0
Active prefixes: 0
Suppressed due to damping: 0
Received external prefixes: 0
Active external prefixes: 0
Externals suppressed: 0
Received internal prefixes: 0
Active internal prefixes: 0
Internals suppressed: 0
RIB State: BGP restart is complete
RIB State: VPN restart is complete

Table bgp.mdt.0
Received prefixes: 0
Accepted prefixes: 0
Active prefixes: 0
Suppressed due to damping: 0
Received external prefixes: 0
Active external prefixes: 0
Externals suppressed: 0
Received internal prefixes: 0
Active internal prefixes: 0
Internals suppressed: 0
RIB State: BGP restart is complete
RIB State: VPN restart is complete

Table VPN-A.inet.0
Received prefixes: 0
Accepted prefixes: 0
Active prefixes: 0
Suppressed due to damping: 0
Received external prefixes: 0
Active external prefixes: 0
Externals suppressed: 0
Received internal prefixes: 0
Active internal prefixes: 0
Internals suppressed: 0
RIB State: BGP restart is complete
RIB State: VPN restart is complete

Table VPN-A.mdt.0
Received prefixes: 0
Accepted prefixes: 0
Active prefixes: 0
Suppressed due to damping: 0
Received external prefixes: 0
Active external prefixes: 0
Externals suppressed: 0
Received internal prefixes: 0
Active internal prefixes: 0
Internals suppressed: 0
RIB State: BGP restart is complete
RIB State: VPN restart is complete
**show bgp group rtf detail**

```plaintext
user@host> show bgp group rtf detail

Group: internal (group-index: 0)
Receive mask: 00000002
Table: bgp.rtarget.0                      Entries: 2
  Target      Mask
  100:100/64  00000002
  200:201/64 (Group)

Group: internal (group-index: 1)
Table: bgp.rtarget.0                      Entries: 1
  Target      Mask
  200:201/64 (Group)
```

**show bgp group summary**

```plaintext
user@host> show bgp group summary

Group: ibgp
Type       Peers     Established  Active/Received/Accepted/Damped
  Internal  3         0

Groups: 1  Peers: 3  External: 0  Internal: 3  Down peers: 3  Flaps: 3
  bgp.13vpn.0  : 0/0/0/0  External: 0/0/0/0  Internal: 0/0/0/0
  bgp.mdt.0   : 0/0/0/0  External: 0/0/0/0  Internal: 0/0/0/0
  VPN-A.inet.0: 0/0/0/0  External: 0/0/0/0  Internal: 0/0/0/0
  VPN-A.mdt.0 : 0/0/0/0  External: 0/0/0/0  Internal: 0/0/0/0
```
**show bgp group traffic-statistics**

**Syntax**

```
show bgp group traffic-statistics
    <brief | detail>
    <group-name>
    <labeled-path label label>
    <logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**labeled-path** option introduced in Junos OS Release 18.1R1 for the MX Series.

**Description**

Display the traffic statistics for configured Border Gateway Protocol (BGP) groups.

**Options**

- **none**—Display traffic statistics for all BGP groups.
- **brief | detail**—(Optional) Display the specified level of output.
- **group-name**—(Optional) Display BGP traffic statistics for only the specified group.
- **labeled-path**—(Optional) Display labeled unicast traffic statistics at the ingress.
- **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 bgp group traffic-statistics (Per-Group-Label Not Configured) on page 1746`
- `show bgp group traffic-statistics (Per-Group-Label Configured) on page 1746`
- `show bgp group traffic-statistics labeled-path (Labeled Unicast) on page 1747`

**Output Fields**

Table 64 on page 1745 describes the output fields for the `show bgp group traffic-statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 64: show bgp group traffic-statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Name of a specific BGP group.</td>
</tr>
<tr>
<td>Group Index</td>
<td>Index number for the BGP group.</td>
</tr>
<tr>
<td>NLRI</td>
<td>Network layer reachability information (NLRI) indicating the source of the traffic statistics for the BGP group.</td>
</tr>
<tr>
<td>FEC</td>
<td>Forwarding equivalence classes (FECs) associated with the BGP group.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets sent through each FEC.</td>
</tr>
</tbody>
</table>
Table 64: show bgp group traffic-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Number of bytes transmitted through each FEC.</td>
</tr>
<tr>
<td>EgressAS</td>
<td>Autonomous system (AS) number of the egress router.</td>
</tr>
<tr>
<td>AdvLabel</td>
<td>Label associated with each FEC.</td>
</tr>
</tbody>
</table>

Sample Output

**show bgp group traffic-statistics (Per-Group-Label Not Configured)**

```
user@host> show bgp group traffic-statistics
Group Name: ext1       Group Index: 0          NLRI: inet-labeled-unicast
<table>
<thead>
<tr>
<th>FEC</th>
<th>Packets</th>
<th>Bytes</th>
<th>EgressAS</th>
<th>AdvLabel</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.55</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100224</td>
</tr>
<tr>
<td>10.255.245.57</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100240</td>
</tr>
<tr>
<td>100.101.0.0</td>
<td>550</td>
<td>48400</td>
<td>25</td>
<td>100256</td>
</tr>
<tr>
<td>100.102.0.0</td>
<td>550</td>
<td>48400</td>
<td>25</td>
<td>100256</td>
</tr>
<tr>
<td>100.103.0.0</td>
<td>550</td>
<td>48400</td>
<td>25</td>
<td>100272</td>
</tr>
<tr>
<td>100.104.0.0</td>
<td>550</td>
<td>48400</td>
<td>25</td>
<td>100272</td>
</tr>
<tr>
<td>192.168.25.0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100288</td>
</tr>
</tbody>
</table>

Group Name: ext2       Group Index: 1          NLRI: inet-labeled-unicast
<table>
<thead>
<tr>
<th>FEC</th>
<th>Packets</th>
<th>Bytes</th>
<th>EgressAS</th>
<th>AdvLabel</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.55</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100224</td>
</tr>
<tr>
<td>10.255.245.57</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100240</td>
</tr>
<tr>
<td>100.101.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100232</td>
</tr>
<tr>
<td>100.102.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100232</td>
</tr>
<tr>
<td>100.103.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100248</td>
</tr>
<tr>
<td>100.104.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100248</td>
</tr>
<tr>
<td>192.168.25.0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100288</td>
</tr>
</tbody>
</table>
```

**show bgp group traffic-statistics (Per-Group-Label Configured)**

```
user@host> show bgp group traffic-statistics
Group Name: ext1       Group Index: 0          NLRI: inet-labeled-unicast
<table>
<thead>
<tr>
<th>FEC</th>
<th>Packets</th>
<th>Bytes</th>
<th>EgressAS</th>
<th>AdvLabel</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.55</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100384</td>
</tr>
<tr>
<td>10.255.245.57</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100400</td>
</tr>
<tr>
<td>100.101.0.0</td>
<td>101</td>
<td>8888</td>
<td>25</td>
<td>100416</td>
</tr>
<tr>
<td>100.102.0.0</td>
<td>101</td>
<td>8888</td>
<td>25</td>
<td>100416</td>
</tr>
<tr>
<td>100.103.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100432</td>
</tr>
<tr>
<td>100.104.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100432</td>
</tr>
<tr>
<td>192.168.25.0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100448</td>
</tr>
</tbody>
</table>

Group Name: ext2       Group Index: 1          NLRI: inet-labeled-unicast
<table>
<thead>
<tr>
<th>FEC</th>
<th>Packets</th>
<th>Bytes</th>
<th>EgressAS</th>
<th>AdvLabel</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.55</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100304</td>
</tr>
<tr>
<td>10.255.245.57</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>100320</td>
</tr>
<tr>
<td>100.101.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100336</td>
</tr>
<tr>
<td>100.102.0.0</td>
<td>0</td>
<td>0</td>
<td>25</td>
<td>100336</td>
</tr>
<tr>
<td>100.103.0.0</td>
<td>101</td>
<td>8888</td>
<td>25</td>
<td>100352</td>
</tr>
</tbody>
</table>
```
### show bgp group traffic-statistics labeled-path (Labeled Unicast)

**user@host> show bgp group traffic-statistics labeled-path**

<table>
<thead>
<tr>
<th>Labels</th>
<th>NextHop</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3(top)</td>
<td>10.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>299840(top)</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110001(top)</td>
<td>40.1.1.1</td>
<td>2</td>
<td>168</td>
</tr>
<tr>
<td>110002</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110003</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110001(top)</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110002</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110003</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>110001(top)</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>120001(top)</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>120002</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>120003</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1000002(top)</td>
<td>40.1.1.1</td>
<td>2</td>
<td>168</td>
</tr>
<tr>
<td>1000003</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1000004</td>
<td>40.1.1.1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### show bgp neighbor

**List of Syntax**
- Syntax on page 1748
- Syntax (EX Series Switch, QFX Series, and OCX Series) on page 1748

#### Syntax

```
show bgp neighbor
  <exact-instance instance-name>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <neighbor-address>
  <output-queue>
  <orf (detail | neighbor-address)
```

#### Syntax (EX Series Switch, QFX Series, and OCX Series)

```
show bgp neighbor
  <instance instance-name>
  <exact-instance instance-name>
  <neighbor-address>
  <orf (neighbor-address | detail)
```

#### 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 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1x53-D20 for the OCX Series.
- orf option introduced in Junos OS Release 9.2.
- exact-instance option introduced in Junos OS Release 11.4.
- output-queue option introduced in Junos OS Release 16.1
- `DontGRHelpFateSharingBfdDown` is added to the options field of the command output in Junos OS Release 18.3R1.

#### Description
Display information about BGP peers.

#### Options
- **none**—Display information about all BGP peers.
- **exact-instance instance-name**—(Optional) Display information for the specified instance only.
- **instance instance-name**—(Optional) Display information about BGP peers for all routing instances whose name begins with this string (for example, `cust1`, `cust11`, and `cust111` are all displayed when you run the `show bgp neighbor instance cust1` command).
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **neighbor-address**—(Optional) Display information for only the BGP peer at the specified IP address.
orf (detail | neighbor-address)—(Optional) Display outbound route-filtering information for all BGP peers or only for the BGP peer at the specified IP address. The default is to display brief output. Use the detail option to display detailed output.

output-queue—(Optional) Display information regarding the number of routes currently queued in the 17 prioritized BGP output queues.

Additional Information
For information about the local-address, nlri, hold-time, and preference statements, see the Junos OS Routing Protocols Library.

Required Privilege Level
view

Related Documentation
- clear bgp neighbor on page 1731

List of Sample Output
- show bgp neighbor on page 1757
- show bgp neighbor (dont-help-shared-fate-bfd-down is configured) on page 1758
- show bgp neighbor (CLNS) on page 1759
- show bgp neighbor (Layer 2 VPN) on page 1760
- show bgp neighbor (Layer 3 VPN) (Not supported on the OCX Series.) on page 1762
- show bgp neighbor neighbor-address on page 1763
- show bgp neighbor neighbor-address (BGP Graceful Restart Enabled) on page 1764
- show bgp neighbor neighbor-address (BGP Long-Lived Graceful Restart) on page 1765
- show bgp neighbor orf neighbor-address detail on page 1765
- show bgp neighbor logical-system on page 1766
- show bgp neighbor output-queue on page 1766
- show bgp neighbor (Segment Routing Traffic Engineering) on page 1767

Output Fields
Table 65 on page 1749 describes the output fields for the show bgp neighbor command. Output fields are listed in the approximate order in which they appear.

Table 65: show bgp neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>Address of the BGP neighbor. The address is followed by the neighbor port number.</td>
</tr>
<tr>
<td>AS</td>
<td>AS number of the peer.</td>
</tr>
<tr>
<td>Local</td>
<td>Address of the local routing device. The address is followed by the peer port number.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of peer: Internal or External.</td>
</tr>
</tbody>
</table>
**Table 65: show bgp neighbor Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Current state of the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connect</strong>—BGP is waiting for the transport protocol connection to be completed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Established</strong>—The BGP session has been established, and the peers are exchanging update messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idle</strong>—This is the first stage of a connection. BGP is waiting for a Start event.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenConfirm</strong>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenSent</strong>—BGP has sent an open message and is waiting to receive an open message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>route reflector client</strong>—The BGP session is established with a route reflector client.</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Internal BGP flags:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Aggregate Label</strong>—BGP has aggregated a set of incoming labels (labels received from the peer) into a single forwarding label.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CleanUp</strong>—The peer session is being shut down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete</strong>—This peer has been deleted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idled</strong>—This peer has been permanently idled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ImportEval</strong>—At the last commit operation, this peer was identified as needing to reevaluate all received routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Initializing</strong>—The peer session is initializing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SendRtn</strong>—Messages are being sent to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sync</strong>—This peer is synchronized with the rest of the peer group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RSync</strong>—This peer in the backup Routing Engine is synchronized with the BGP peer in the master Routing Engine for nonstop active routing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TryConnect</strong>—Another attempt is being made to connect to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unconfigured</strong>—This peer is not configured.</td>
</tr>
<tr>
<td></td>
<td>• <strong>WriteFailed</strong>—An attempt to write to this peer failed.</td>
</tr>
<tr>
<td><strong>Last state</strong></td>
<td>Previous state of the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connect</strong>—BGP is waiting for the transport protocol connection to be completed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Established</strong>—The BGP session has been established, and the peers are exchanging update messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idle</strong>—This is the first stage of a connection. BGP is waiting for a Start event.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenConfirm</strong>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</td>
</tr>
</tbody>
</table>
|            | • **OpenSent**—BGP has sent an open message and is waiting to receive an open message from the peer.
### Table 65: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last event</strong></td>
<td>Last activity that occurred in the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• Closed—The BGP session closed.</td>
</tr>
<tr>
<td></td>
<td>• ConnectRetry—The transport protocol connection failed, and BGP is trying again to connect.</td>
</tr>
<tr>
<td></td>
<td>• HoldTime—The session ended because the hold timer expired.</td>
</tr>
<tr>
<td></td>
<td>• KeepAlive—The local routing device sent a BGP keepalive message to the peer.</td>
</tr>
<tr>
<td></td>
<td>• Open—The local routing device sent a BGP open message to the peer.</td>
</tr>
<tr>
<td></td>
<td>• OpenFail—The local routing device did not receive an acknowledgment of a BGP open message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• RecvKeepAlive—The local routing device received a BGP keepalive message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• RecvNotify—The local routing device received a BGP notification message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• RecvOpen—The local routing device received a BGP open message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• RecvUpdate—The local routing device received a BGP update message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• Start—The peering session started.</td>
</tr>
<tr>
<td></td>
<td>• Stop—The peering session stopped.</td>
</tr>
<tr>
<td></td>
<td>• TransportError—A TCP error occurred.</td>
</tr>
<tr>
<td><strong>Last error</strong></td>
<td>Last error that occurred in the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• Cease—An error occurred, such as a version mismatch, that caused the session to close.</td>
</tr>
<tr>
<td></td>
<td>• Finite State Machine Error—In setting up the session, BGP received a message that it did not understand.</td>
</tr>
<tr>
<td></td>
<td>• Hold Time Expired—The session's hold time expired.</td>
</tr>
<tr>
<td></td>
<td>• Message Header Error—The header of a BGP message was malformed.</td>
</tr>
<tr>
<td></td>
<td>• Open Message Error—A BGP open message contained an error.</td>
</tr>
<tr>
<td></td>
<td>• None—No errors occurred in the BGP session.</td>
</tr>
<tr>
<td></td>
<td>• Update Message Error—A BGP update message contained an error.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Name of the export policy that is configured on the peer.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Name of the import policy that is configured on the peer.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Options</td>
<td>Configured BGP options:</td>
</tr>
<tr>
<td></td>
<td>• AddressFamily—Configured address family: inet or inet-vpn.</td>
</tr>
<tr>
<td></td>
<td>• AdvertiseBGPStatic—Configured BGP static routes are advertised.</td>
</tr>
<tr>
<td></td>
<td>• AuthKeyChain—Authentication key change is enabled.</td>
</tr>
<tr>
<td></td>
<td>• BfdEnabled—Status of BFD.</td>
</tr>
<tr>
<td></td>
<td>• DontGRHelpFateSharingBfdDown—Status of the dont-help-shared-fate-bfd-down option. If this option is configured the device does not go into graceful restart helper mode.</td>
</tr>
<tr>
<td></td>
<td>• DropPathAttributes—Certain path attributes are configured to be dropped from neighbor updates during inbound processing.</td>
</tr>
<tr>
<td></td>
<td>• GracefulRestart—Graceful restart is configured.</td>
</tr>
<tr>
<td></td>
<td>• HoldTime—Hold time configured with the hold-time statement. The hold time is three times the interval at which keepalive messages are sent.</td>
</tr>
<tr>
<td></td>
<td>• IgnorePathAttributes—Certain path attributes are configured to be ignored in neighbor updates during inbound processing.</td>
</tr>
<tr>
<td></td>
<td>• Local Address—Address configured with the local-address statement.</td>
</tr>
<tr>
<td></td>
<td>• LLGR—BGP long-lived graceful restart capability is configured.</td>
</tr>
<tr>
<td></td>
<td>• LLGRHelperDisabled—BGP long-lived graceful restart is completely disabled for a neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Multihop—Allow BGP connections to external peers that are not on a directly connected network.</td>
</tr>
<tr>
<td></td>
<td>• NLRI—Configured MBGP state for the BGP group: multicast, unicast, or both if you have configured nlri any.</td>
</tr>
<tr>
<td></td>
<td>• Peer AS—Configured peer autonomous system (AS).</td>
</tr>
<tr>
<td></td>
<td>• Preference—Preference value configured with the preference statement.</td>
</tr>
<tr>
<td></td>
<td>• Refresh—Configured to refresh automatically when the policy changes.</td>
</tr>
<tr>
<td></td>
<td>• Rib-group—Configured routing table group.</td>
</tr>
<tr>
<td></td>
<td>• RFC6514CompliantSafi129—Configured SAFI 129 according to RFC 6514 (BGP VPN multicast used to use SAFI 128).</td>
</tr>
<tr>
<td>Path-attributes dropped</td>
<td>Path attribute codes that are dropped from neighbor updates.</td>
</tr>
<tr>
<td>Path-attributes ignored</td>
<td>Path attribute codes that are ignored during neighbor updates.</td>
</tr>
<tr>
<td>Peer does not support</td>
<td>BGP neighbor does not support long-lived graceful restart (LLGR) restarter mode completely.</td>
</tr>
<tr>
<td>LLGR Restarter or</td>
<td></td>
</tr>
<tr>
<td>Receiver functionality</td>
<td></td>
</tr>
<tr>
<td>Peer does not support</td>
<td>BGP neighbor does not support long-lived graceful restart (LLGR) restarter mode for any family.</td>
</tr>
<tr>
<td>LLGR Restarter</td>
<td></td>
</tr>
<tr>
<td>functionality</td>
<td></td>
</tr>
<tr>
<td>Authentication key</td>
<td>(Appears only if the authentication-keychain statement has been configured) Name of the authentication keychain enabled.</td>
</tr>
<tr>
<td>change</td>
<td></td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>(Appears only if the authentication-algorithm statement has been configured) Type of authentication algorithm enabled: hmac or md5.</td>
</tr>
</tbody>
</table>
### Table 65: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address families configured</td>
<td>Names of configured address families for the VPN.</td>
</tr>
<tr>
<td>BGP-Static Advertisement Policy</td>
<td>Name of the BGP static policy that is configured on the peer.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Address of the local routing device.</td>
</tr>
<tr>
<td>Remove-private options</td>
<td>Options associated with the <code>remove-private</code> statement.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Hold time configured with the <code>hold-time</code> statement. The hold time is three times</td>
</tr>
<tr>
<td></td>
<td>the interval at which keepalive messages are sent.</td>
</tr>
<tr>
<td>Flags for NLRI</td>
<td>Flags related to labeled-unicast:</td>
</tr>
<tr>
<td></td>
<td>• TrafficStatistics—Collection of statistics for labeled-unicast traffic is enabled.</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Information about labeled-unicast traffic statistics:</td>
</tr>
<tr>
<td></td>
<td>• Options—Options configured for collecting statistics about labeled-unicast traffic.</td>
</tr>
<tr>
<td></td>
<td>• File—Name and location of statistics log files.</td>
</tr>
<tr>
<td></td>
<td>• size—Size of all the log files, in bytes.</td>
</tr>
<tr>
<td></td>
<td>• files—Number of log files.</td>
</tr>
<tr>
<td>Traffic Statistics Interval</td>
<td>Time between sample periods for labeled-unicast traffic statistics, in seconds.</td>
</tr>
<tr>
<td>Preference</td>
<td>Preference value configured with the <code>preference</code> statement.</td>
</tr>
<tr>
<td>Outbound Timer</td>
<td>Time for which the route is available in Junos OS routing table before it is</td>
</tr>
<tr>
<td></td>
<td>exported to BGP. This field is displayed in the output only if the <code>out-delay</code></td>
</tr>
<tr>
<td></td>
<td>parameter is configured to a non-zero value.</td>
</tr>
<tr>
<td>Number of flaps</td>
<td>Number of times the BGP session has gone down and then come back up.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>Router identifier of the peer.</td>
</tr>
<tr>
<td>Group index</td>
<td>Index number for the BGP peer group. The index number differentiates between</td>
</tr>
<tr>
<td></td>
<td>groups when a single BGP group is split because of different configuration options</td>
</tr>
<tr>
<td></td>
<td>at the group and peer levels.</td>
</tr>
<tr>
<td>Peer index</td>
<td>Index that is unique within the BGP group to which the peer belongs.</td>
</tr>
<tr>
<td>Local ID</td>
<td>Router identifier of the local routing device.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the interface on the local routing device.</td>
</tr>
<tr>
<td>Active holdtime</td>
<td>Hold time that the local routing device negotiated with the peer.</td>
</tr>
<tr>
<td>Keepalive Interval</td>
<td>Keepalive interval, in seconds.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>BFD</strong></td>
<td>Status of BFD failure detection.</td>
</tr>
<tr>
<td><strong>Local Address</strong></td>
<td>Name of directly connected interface over which direct EBGP peering is established.</td>
</tr>
<tr>
<td><strong>NLRI and times for LLGR configured on peer</strong></td>
<td>Names of address families and stale time for BGP long-lived graceful restart configured on the BGP peer or neighbor.</td>
</tr>
<tr>
<td></td>
<td>Times are displayed using the routing protocol daemon (rpd) %#0T format: &lt;weeks&gt;w&lt;days&gt;d&lt;hours&gt;:&lt;minutes&gt;:&lt;seconds&gt;</td>
</tr>
<tr>
<td></td>
<td>Zero leading elements are omitted, for example, a value less than one week do not include the weeks.</td>
</tr>
<tr>
<td><strong>NLRI and times that peer supports LLGR Restarter for</strong></td>
<td>Names of address families and stale time that the BGP peer supports for restarter mode for BGP long-lived graceful restart.</td>
</tr>
<tr>
<td></td>
<td>Times are displayed using the routing protocol daemon (rpd) %#0T format: &lt;weeks&gt;w&lt;days&gt;d&lt;hours&gt;:&lt;minutes&gt;:&lt;seconds&gt;</td>
</tr>
<tr>
<td></td>
<td>Zero leading elements are omitted, for example, a value less than one week do not include the weeks.</td>
</tr>
<tr>
<td><strong>NLRI that peer saved LLGR forwarding for</strong></td>
<td>Name of the address family for which the BGP peer saved BGP long-lived graceful restart forwarding.</td>
</tr>
<tr>
<td><strong>Graceful Restart Details</strong></td>
<td>Amount of time that is remaining until LLGR expires and the time remaining on the GR stale timer, along with RIB details, are displayed while LLGR receiver mode is active (a peer that negotiated LLGR has disconnected and not yet reconnected).</td>
</tr>
<tr>
<td><strong>NLRI we are holding stale routes for</strong></td>
<td>Names of address families (NLRI$s) for which that stale routes are held or preserved when BGP graceful restart receiver mode is active for a neighbor.</td>
</tr>
<tr>
<td><strong>Time until end-of-rib is assumed for stale routes</strong></td>
<td>Amount of time remaining on the stale timer until which end-of-RIB (EoR) markers are assumed when BGP graceful restart receiver mode is active for a neighbor.</td>
</tr>
<tr>
<td></td>
<td>Time is displayed in Coordinated Universal Time (UTC) format (YYYY-MM-DD-HH:MM:SS). Note that the stale timer display (‘Time until end-of-rib is assumed’) is also present when a session is active, but the neighbor as not yet sent all of the end-of-rib indications.</td>
</tr>
<tr>
<td><strong>Time until stale routes are deleted or become long-lived stale</strong></td>
<td>Amount of time up to which stale routes are deleted or become long-lived stale routes when BGP graceful restart receiver mode is active for a neighbor.</td>
</tr>
<tr>
<td><strong>NLRI for restart configured on peer</strong></td>
<td>Names of address families configured for restart.</td>
</tr>
<tr>
<td><strong>NLRI advertised by peer</strong></td>
<td>Address families supported by the peer: unicast or multicast.</td>
</tr>
<tr>
<td><strong>NLRI for this session</strong></td>
<td>Address families being used for this session.</td>
</tr>
<tr>
<td><strong>Peer supports Refresh capability</strong></td>
<td>Remote peer’s ability to send and request full routing table readvertisement (route refresh capability). For more information, see RFC 2918, Route Refresh Capability for BGP-4.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Restart time configured on peer</td>
<td>Configured time allowed for restart on the neighbor.</td>
</tr>
<tr>
<td>Stale routes from peer are kept for</td>
<td>When graceful restart is negotiated, the maximum time allowed to hold routes from neighbors after the BGP session has gone down.</td>
</tr>
<tr>
<td>Peer does not support Restarter functionality</td>
<td>Graceful restart recaster-mode is disabled on the peer.</td>
</tr>
<tr>
<td>Peer does not support Receiver functionality</td>
<td>Graceful restart helper-mode is disabled on the peer.</td>
</tr>
<tr>
<td>Restart time requested by this peer</td>
<td>Restart time requested by this neighbor during capability negotiation.</td>
</tr>
<tr>
<td>Restart flag received from the peer</td>
<td>When this field appears, the BGP speaker has restarted (Restarting), and this peer should not wait for the end-of-rib marker from the speaker before advertising routing information to the speaker.</td>
</tr>
<tr>
<td>NLRI that peer supports restart for</td>
<td>Neighbor supports graceful restart for this address family.</td>
</tr>
<tr>
<td>NLRI peer can save forwarding state</td>
<td>Neighbor supporting this address family saves all forwarding states.</td>
</tr>
<tr>
<td>NLRI that peer saved forwarding for</td>
<td>Neighbor saves all forwarding states for this address family.</td>
</tr>
<tr>
<td>NLRI that restart is negotiated for</td>
<td>Router supports graceful restart for this address family.</td>
</tr>
<tr>
<td>NLRI of received end-of-rib markers</td>
<td>Address families for which end-of-routing-table markers are received from the neighbor.</td>
</tr>
<tr>
<td>NLRI of all end-of-rib markers sent</td>
<td>Address families for which end-of-routing-table markers are sent to the neighbor.</td>
</tr>
<tr>
<td>Peer supports 4 byte AS extension (peer-as1)</td>
<td>Peer understands 4-byte AS numbers in BGP messages. The peer is running Junos OS Release 9.1 or later.</td>
</tr>
<tr>
<td>NLRIs for which peer can receive multiple paths</td>
<td>Appears in the command output of the local router if the downstream peer is configured to receive multiple BGP routes to a single destination, instead of only receiving the active route. Possible value is inet-unicast.</td>
</tr>
<tr>
<td>NLRIs for which peer can send multiple paths: inet-unicast</td>
<td>Appears in the command output of the local router if the upstream peer is configured to send multiple BGP routes to a single destination, instead of only sending the active route. Possible value is inet-unicast.</td>
</tr>
</tbody>
</table>
Table 65: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table inet.number</td>
<td>Information about the routing table:</td>
</tr>
<tr>
<td></td>
<td>• RIB State—BGP is in the graceful restart process for this routing table: restart is complete or restart in progress.</td>
</tr>
<tr>
<td></td>
<td>• Bit—Number that represents the entry in the routing table for this peer.</td>
</tr>
<tr>
<td></td>
<td>• Send state—State of the BGP group: in sync, not in sync, or not advertising.</td>
</tr>
<tr>
<td></td>
<td>• Active prefixes—Number of prefixes received from the peer that are active in the routing table.</td>
</tr>
<tr>
<td></td>
<td>• Received prefixes—Total number of prefixes from the peer, both active and inactive, that are in the routing table.</td>
</tr>
<tr>
<td></td>
<td>• Accepted prefixes—Total number of prefixes from the peer that have been accepted by a routing policy.</td>
</tr>
<tr>
<td></td>
<td>• Suppressed due to damping—Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
</tr>
<tr>
<td>Last traffic (seconds)</td>
<td>Last time any traffic was received from the peer or sent to the peer, and the last time the local routing device checked.</td>
</tr>
<tr>
<td>Input messages</td>
<td>Messages that BGP has received from the receive socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.</td>
</tr>
<tr>
<td>Output messages</td>
<td>Messages that BGP has written to the transmit socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.</td>
</tr>
<tr>
<td>Input dropped path attributes</td>
<td>Information about dropped path attributes:</td>
</tr>
<tr>
<td></td>
<td>• Code—Path attribute code.</td>
</tr>
<tr>
<td></td>
<td>• Count—Path attribute count.</td>
</tr>
<tr>
<td>Input ignored path attributes</td>
<td>Information about ignored path attributes:</td>
</tr>
<tr>
<td></td>
<td>• Code—Path attribute code.</td>
</tr>
<tr>
<td></td>
<td>• Count—Path attribute count.</td>
</tr>
<tr>
<td>Output queue</td>
<td>Number of BGP packets that are queued to be transmitted to a particular neighbor for a particular routing table. Output queue 0 is for unicast NLRI, and queue 1 is for multicast NLRI.</td>
</tr>
<tr>
<td></td>
<td>It also specifies the routing table name and the NLRI that the table was advertised through, in the format (routing table name, NLRI).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The output queue of routing tables that are not advertised, will only show up at <strong>extensive</strong> output level.</td>
</tr>
<tr>
<td>Trace options</td>
<td>Configured tracing of BGP protocol packets and operations.</td>
</tr>
<tr>
<td>Trace file</td>
<td>Name of the file to receive the output of the tracing operation.</td>
</tr>
</tbody>
</table>
Table 65: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Updates recv</td>
<td>(orf option only) Number of outbound-route filters received for each configured address family. The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</td>
</tr>
<tr>
<td>Immediate</td>
<td>(orf option only) Number of route updates received with the immediate flag set. The immediate flag indicates that the BGP peer should readvertise the updated routes.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</td>
</tr>
<tr>
<td>Filter</td>
<td>(orf option only) Type of prefix filter received: prefix-based or extended-community.</td>
</tr>
<tr>
<td>Received filter entries</td>
<td>(orf option only) List of received filters displayed.</td>
</tr>
<tr>
<td>seq</td>
<td>(orf option only) Numerical order assigned to this prefix entry among all the received outbound route filter prefix entries.</td>
</tr>
<tr>
<td>prefix</td>
<td>(orf option only) Address for the prefix entry that matches the filter.</td>
</tr>
<tr>
<td>minlength</td>
<td>(orf option only) Minimum prefix length, in bits, required to match this prefix.</td>
</tr>
<tr>
<td>maxlength</td>
<td>(orf option only) Maximum prefix length, in bits, required to match this prefix.</td>
</tr>
<tr>
<td>match</td>
<td>(orf option only) For this prefix match, whether to permit or deny route updates.</td>
</tr>
</tbody>
</table>

Sample Output
show bgp neighbor

user@host > show bgp neighbor

For M Series, MX Series, and T Series routers running Junos OS Release 16.1 or later, the show bgp neighbor output includes the BGP group the peer belongs to, the routing instance (if any) that the peer is configured in, and the routing instance that the peer is using for the forwarding context (if applicable). An example follows.

Peer: 10.255.7.250+179 AS 10  Local: 10.255.7.248+63740 AS 10
Group: toAsbr2           Routing-Instance: master
Forwarding routing-instance: toAs2
  Type: Internal        State: Established      Flags: <Sync>
Last State: OpenConfirm Last Event: RecvKeepAlive
Last Error: None
Export: [ redist_static ]
Options: <Preference LocalAddress PeerAS Refresh>
Options: <AdvertiseBGPStatic>
Local Address: 10.255.7.248 Holdtime: 90 Preference: 170 Outbound Timer: 50
Number of flaps: 0
Peer ID: 10.255.7.250    Local ID: 10.255.7.248    Active Holdtime: 90
Keepalive Interval: 30   Group index: 0    Peer index: 0
BFD: disabled, down
NLRI for restart configured on peer: inet-unicast
NLRI advertised by peer: inet-unicast
NLRI for this session: inet-unicast
Peer supports Refresh capability (2)
Stale routes from peer are kept for: 300
Peer does not support Restarter functionality
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer supports 4 byte AS extension (peer-as 10)
Peer does not support Addpath
NLRI that we support extended nexthop encoding for: inet-unicast
NLRI that peer supports extended nexthop encoding for: inet-unicast

Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes: 1
  Received prefixes: 1
  Accepted prefixes: 1
  Suppressed due to damping: 0
  Advertised prefixes: 1
  Last traffic (seconds): Received 9 Sent 5 Checked 5
  Input messages: Total 36 Updates 2 Refreshes 0 Octets 718
  Output messages: Total 37 Updates 1 Refreshes 0 Octets 796
  Output Queue[0]: 0 (inet.0, inet-unicast)

Peer: 10.255.162.214+52193 AS 100 Local: 10.255.167.205+179 AS 100
  Type: Internal State: Established (route reflector client) Flags: <Sync>
  Last State: OpenConfirm Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress Cluster AddressFamily Rib-group Refresh>
  Address families configured: inet-unicast inet-vpn-unicast route-target
  Local Address: 10.255.167.205 Holdtime: 90 Preference: 170
  Number of flaps: 0
  Peer ID: 10.255.162.214 Local ID: 10.255.167.205 Active Holdtime: 90
  Keepalive Interval: 30 Group index: 0 Peer index: 1

show bgp neighbor (dont-help-shared-fate-bfd-down is configured)

user@host> show bgp neighbor

Peer: 10.1.1.1 AS 200 Local: unspecified AS 17
  Group: one Routing-Instance: master
  Forwarding routing-instance: master
  Type: External State: Idle Flags: <PeerInterfaceError>
  Last State: NoState Last Event: NoEvent
  Last Error: None
  Options: <Preference PeerAS Refresh>
  Options: <BfdEnabled>
  Options: <DontGRHelpFateSharingBfdDown>
  Holdtime: 90 Preference: 170
  Number of flaps: 0
  Trace options: bridge
  Trace file: /var/log/bgp-log size 131072 files 10

Peer: 20.1.1.1 AS 200 Local: unspecified AS 17
  Group: one Routing-Instance: master
Forwarding routing-instance: master
  Type: External  State: Idle  Flags: <PeerInterfaceError>
  Last State: NoState  Last Event: NoEvent
  Last Error: None
  Options: <Preference PeerAS Refresh>
  Options: <BfdEnabled>
  Options: <DontGRHelpFateSharingBfdDown>
  Holdtime: 90  Preference: 170
  Number of flaps: 0
  Trace options: bridge
  Trace file: /var/log/bgp-log size 131072 files 10

Peer: 30.1.1.1 AS 200  Local: unspecified AS 17
  Group: two  Routing-Instance: master
Forwarding routing-instance: master
  Type: External  State: Idle  Flags: <PeerInterfaceError>
  Last State: NoState  Last Event: NoEvent
  Last Error: None
  Options: <Preference PeerAS Refresh>
  Options: <BfdEnabled>
  Options: <DontGRHelpFateSharingBfdDown>
  Holdtime: 90  Preference: 170
  Number of flaps: 0
  Trace options: bridge
  Trace file: /var/log/bgp-log size 131072 files 10

show bgp neighbor (CLNS)

user@host> show bgp neighbor

Peer: 10.245.245.1+179 AS 200  Local: 10.245.245.3+3770 AS 100
  Type: External  State: Established  Flags: <ImportEval Sync>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: None
  Options: <Multihop Preference LocalAddress HoldTime AddressFamily PeerAS Rib-group Refresh>
  Address families configured: iso-vpn-unicast
  Local Address: 10.245.245.3 Holdtime: 90  Preference: 170
  Number of flaps: 0
  Peer ID: 10.245.245.1  Local ID: 10.245.245.3  Active Holdtime: 90
  Keepalive Interval: 30  Peer index: 0
  NLRI advertised by peer: iso-vpn-unicast
  NLRI for this session: iso-vpn-unicast
  Peer supports Refresh capability (2)
  Table bgp.isovpn.0 Bit: 10000
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
    Send state: in sync
    Active prefixes: 3
    Received prefixes: 3
    Suppressed due to damping: 0
    Advertised prefixes: 3
  Table aaaa.iso.0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
    Send state: not advertising
    Active prefixes: 3
    Received prefixes: 3
    Suppressed due to damping: 0
    Last traffic (seconds): Received 6  Sent 5  Checked 5
show bgp neighbor (Layer 2 VPN)

user@host> show bgp neighbor

Peer: 10.69.103.2     AS 65536 Local: 10.69.103.1     AS 65539
Type: External    State: Active         Flags: <ImportEval>
Last State: Idle          Last Event: Start
Last Error: None
Export: [ BGP-INET-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
Address families configured: inet-unicast
Local Address: 10.69.103.1 Holdtime: 90 Preference: 170
Number of flaps: 0

Peer: 10.69.104.2     AS 65539 Local: 10.69.104.1     AS 65539
Type: External    State: Active         Flags: <ImportEval>
Last State: Idle          Last Event: Start
Last Error: None
Export: [ BGP-L-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS Refresh>
Address families configured: inet-labeled-unicast
Local Address: 10.69.104.1 Holdtime: 90 Preference: 170
Number of flaps: 0

Type: Internal    State: Established    Flags: <ImportEval>
Last State: OpenConfirm   Last Event: RecvKeepAlive
Last Error: None
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily Rib-group Refresh>
Address families configured: inet-vpn-unicast l2vpn
Keepalive Interval: 30
NLRI for restart configured on peer: inet-vpn-unicast l2vpn
NLRI advertised by peer: inet-vpn-unicast l2vpn
NLRI for this session: inet-vpn-unicast l2vpn
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-vpn-unicast l2vpn
NLRI peer can save forwarding state: inet-vpn-unicast l2vpn
NLRI that peer saved forwarding for: inet-vpn-unicast l2vpn
NLRI that restart is negotiated for: inet-vpn-unicast l2vpn
NLRI of received end-of-rib markers: inet-vpn-unicast l2vpn
Table bgp.l3vpn.0 Bit: 10000
RIB State: BGP restart in progress
RIB State: VPN restart in progress
Send state: in sync
Active prefixes: 10
Received prefixes: 10
Suppressed due to damping: 0
Table bgp.l2vpn.0 Bit: 20000
<table>
<thead>
<tr>
<th>Table</th>
<th>Prefixes</th>
<th>Damping</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP-INET</td>
<td>Active: 1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Received: 1</td>
<td></td>
</tr>
<tr>
<td>L2VPN.l2vpn.0</td>
<td>Active: 1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Received: 1</td>
<td></td>
</tr>
</tbody>
</table>

Last traffic (seconds): Received 0    Sent 0    Checked 0
Input messages: Total 14    Updates 13    Refreshes 0    Octets 1053
Output messages: Total 3    Updates 0    Refreshes 0    Octets 105
show bgp neighbor (Layer 3 VPN) (Not supported on the OCX Series.)

```
user@host> show bgp neighbor

Peer: 192.0.2.0.179 AS 10045 Local: 192.0.2.1+1214 AS 10045
Type: Internal State: Established Flags: <ImportEval>
Last State: OpenConfirm Last Event: RecvKeepAlive
Last Error: None
Export: [ match-all ] Import: [ match-all ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily
Rib-group Refresh>
Address families configured: inet-vpn-unicast
Local Address: 192.0.2.1 Holdtime: 90 Preference: 170
Flags for NLRI inet-labeled-unicast: TrafficStatistics
Traffic Statistics: Options: all File: /var/log/bstat.log
size 131072 files 10
Traffic Statistics Interval: 60
Number of flaps: 0
Peer ID: 192.168.1.110 Local ID: 192.168.1.111 Active Holdtime: 90
Keepalive Interval: 30
NLRI for restart configured on peer: inet-vpn-unicast
NLRI advertised by peer: inet-vpn-unicast
NLRI for this session: inet-vpn-unicast
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-vpn-unicast
NLRI peer can save forwarding state: inet-vpn-unicast
NLRI that peer saved forwarding for: inet-vpn-unicast
NLRI that restart is negotiated for: inet-vpn-unicast
NLRI of received end-of-rib markers: inet-vpn-unicast
NLRI of all end-of-rib markers sent: inet-vpn-unicast
```

Table bgp.l3vpn.0 Bit: 10000
RIB State: BGP restart is complete
Send state: in sync
Active prefixes: 2
Received prefixes: 2
Suppressed due to damping: 0

Table vpn-green.inet.0 Bit: 20001
RIB State: BGP restart is complete
Send state: in sync
Active prefixes: 2
Received prefixes: 2
Suppressed due to damping: 0

Last traffic (seconds): Received 15  Sent 20  Checked 20
Input messages: Total 40  Updates 2  Refreshes 0  Octets 856
Output messages: Total 44  Updates 2  Refreshes 0  Octets 1066
Output Queue[0]: 0 (bgp.l3vpn.0, inet-vpn-unicast)
Output Queue[1]: 0 (vpn-green.inet.0, inet-vpn-unicast)
show bgp neighbor neighbor-address

<table>
<thead>
<tr>
<th>Peer: 10.255.245.12</th>
<th>AS 35</th>
<th>Local: 10.255.245.13</th>
<th>AS 35</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: Internal</td>
<td>State: Established (route reflector client)</td>
<td>Flags: &lt;Sync&gt;</td>
<td></td>
</tr>
<tr>
<td>Last State: OpenConfirm</td>
<td>Last Event: RecvKeepAlive</td>
<td>Last Error: None</td>
<td></td>
</tr>
<tr>
<td>Options:</td>
<td>&lt;Preference LocalAddress HoldTime Cluster AddressFamily Rib-group Refresh&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options: RFC6514CompliantSafi129</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address families configured: inet-vpn-unicast inet-labeled-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Address: 10.255.245.13</td>
<td>Holdtime: 90</td>
<td>Preference: 170</td>
<td></td>
</tr>
<tr>
<td>Flags for NLRI inet-vpn-unicast: AggregateLabel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags for NLRI inet-labeled-unicast: AggregateLabel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of flaps: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer ID: 10.255.245.12</td>
<td>Local ID: 10.255.245.13</td>
<td>Active Holdtime: 90</td>
<td></td>
</tr>
<tr>
<td>Keepalive Interval: 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BFD: disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI advertised by peer: inet-vpn-unicast inet-labeled-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI for this session: inet-vpn-unicast inet-labeled-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer supports Refresh capability (2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart time configured on the peer: 300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stale routes from peer are kept for: 60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restart time requested by this peer: 300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI that peer supports restart for: inet-unicast inet6-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI that restart is negotiated for: inet-unicast inet6-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI of received end-of-rib markers: inet-unicast inet6-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLRI of all end-of-rib markers sent: inet-unicast inet6-unicast</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table inet.0 Bit: 10000
  RIB State: restart is complete
  Send state: in sync
  Active prefixes: 4
  Received prefixes: 6
  Suppressed due to damping: 0

Table inet6.0 Bit: 20000
  RIB State: restart is complete
  Send state: in sync
  Active prefixes: 0
  Received prefixes: 2
  Suppressed due to damping: 0

Last traffic (seconds): Received 3  Sent 3  Checked 3
Input messages: Total 9  Updates 6  Refreshes 0  Octets 403
Output messages: Total 7  Updates 3  Refreshes 0  Octets 365
Output Queue[0]: 0 (inet.0, inet-unicast)
Output Queue[1]: 0 (inet6.0, inet6-unicast)
Trace options: detail packets
Trace file: /var/log/bgpgr.size 131072 files 10

show bgp neighbor neighbor-address

<table>
<thead>
<tr>
<th>Peer: 192.168.4.222+4902</th>
<th>AS 65501</th>
<th>Local: 192.168.4.221+179</th>
<th>AS 65500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: External</td>
<td>State: Established</td>
<td>Flags: &lt;Sync&gt;</td>
<td></td>
</tr>
<tr>
<td>Last State: OpenConfirm</td>
<td>Last Event: RecvKeepAlive</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
show bgp neighbor neighbor-address (BGP Graceful Restart Enabled)

user@router> show bgp neighbor 10.255.255.16

Peer: 10.255.255.16 AS 100  Local: 10.255.255.12 AS 100
Type: Internal  State: Active  Flags: <>
Last State: Idle  Last Event: Start
Last Error: None
Options: <Preference LocalAddress AddressFamily Rib-group Refresh>
Options: <LLGR>
Address families configured: l2vpn
Local Address: 10.255.255.12 Holdtime: 90 Preference: 170
L2VPN:
Number of flaps: 6
Last flap event: Restart
NLRI we are holding stale routes for: inet-vpn-unicast
Time until stale routes are deleted or become long-lived stale: 00:01:57
Time until end-of-rib is assumed for stale routes: 00:04:43
Table bgp.l3vpn.0
  RIB State: BGP restart is complete
show bgp neighbor neighbor-address (BGP Long-Lived Graceful Restart)

user@router> show bgp neighbor 10.4.12.11

Peer: 10.4.12.11 AS 100        Local: 10.6.128.225 AS 100
Type: Internal    State: Active         Flags: <>
Last State: Idle          Last Event: Start
Last Error: None
Export: [ foo ]
Options: <Preference LocalAddress Refresh GracefulRestart>
Options: <LLGR>
Local Address: 10.6.128.225 Holdtime: 90 Preference: 170
Number of flaps: 3
Last flap event: Restart
Error: 'Cease' Sent: 0 Recv: 1
Time until long-lived stale routes deleted: inet-vpn-unicast 10:00:22
route-target 10:00:22
Table bgp.l3vpn.0
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: not advertising
  Active prefixes:  0
  Received prefixes:  7
  Accepted prefixes:  7
  Suppressed due to damping:  0
Table foo.inet.0 Bit: 30000
  RIB State: VPN restart is complete
  Send state: not in sync
  Active prefixes:  0
  Received prefixes:  7
  Accepted prefixes:  7
  Suppressed due to damping:  0

show bgp neighbor orf neighbor-address detail

user@host > show bgp neighbor orf 192.168.165.56 detail

Peer: 192.168.165.56+179 Type: External
Group: ext1
inet-unicast
  Filter updates recv:  1 Immediate:  1
Filter: prefix-based receive
  Received filter entries:
  seq 1: prefix 2.2.2.2/32: minlen 32: maxlen 32: match deny:

inet6-unicast
  Filter updates recv: 0 Immediate: 1

Filter: prefix-based receive
  Received filter entries:

show bgp neighbor logical-system

user@host > show bgp neighbor logical-system ITR1

Peer: 10.79.8.2+179 AS 65536   Local: 10.79.8.1+50891 AS 65500
  Description: MX1
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  ....
  Table inet.0 Bit: 10000
  Send state: in sync
  Active prefixes: 1
  Received prefixes: 1
  Accepted prefixes: 1
  Suppressed due to damping: 0
  Advertised prefixes: 10
  Stale prefixes: 4: <=new, line only appears if count is non-0
  It is the Number of prefixes marked as stale;
  LLGR-stale prefixes: 5: <=new, line only appears if count is non-0
  It is the Number of prefixes marked as LLGR-stale

show bgp neighbor output-queue

user@host > show bgp neighbor output-queue

Peer: 192.0.2.2+179 AS 103   Local: 192.0.2.1+50799 AS 102
  Output Queue[0]: 0   (inet.0, inet-unicast)
    Priority 1: 0
    Priority 2: 0
    Priority 3: 0
    Priority 4: 0
    Priority 5: 0
    Priority 6: 0
    Priority 7: 0
    Priority 8: 0
    Priority 9: 0
    Priority 10: 0
    Priority 11: 0
    Priority 12: 0
    Priority 13: 0
    Priority 14: 0
    Priority 15: 0
    Priority 16: 0
    Expedited: 0
### show bgp neighbor (Segment Routing Traffic Engineering)

```plaintext
user@host > show bgp neighbor

run show bgp neighbor 1.1.1.254

  Peer: 1.1.1.254+60180 AS 100   Local: 1.1.1.1+179 AS 100
  Group: toB                   Routing-Instance: master
  Forwarding routing-instance: master
  Type: Internal    State: Established    Flags: <Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: <Preference LocalAddress>
  Address families configured: inet-segment-routing-te
  Local Address: 1.1.1.1 Holdtime: 90 Preference: 170 Local AS: 100 Local System
  AS: 0
  Number of flaps: 0
  Peer ID: 128.9.150.15   Local ID: 128.9.150.110     Active Holdtime: 90
  Keepalive Interval: 30   Group index: 0    Peer index: 0
  I/O Session Thread: bgpio-0 State: Enabled
  BFD: disabled, down
  NLRI for restart configured on peer: inet-segment-routing-te
  NLRI advertised by peer: inet-segment-routing-te
  NLRI for this session: inet-segment-routing-te
  Peer supports Refresh capability (2)
  Stale routes from peer are kept for: 300
  Peer does not support Restarter functionality
  Restart flag received from the peer: Notification
  NLRI that restart is negotiated for: inet-segment-routing-te
  Peer does not support LLGR Restarter functionality
  Peer supports 4 byte AS extension (peer-as 100)
  Peer does not support Addpath
  Last traffic (seconds): Received 17628 Sent 25  Checked 17628
  Input messages:  Total 2       Updates 0       Refreshes 0     Octets 82
  Output messages: Total 1       Updates 0       Refreshes 0     Octets 19
  Trace options: all
  Trace file: /var/log/bgp.log size 10485760 files 10
```
**show bgp replication**

**Syntax**

show bgp replication

**Release Information**

Command introduced in Junos OS Release 8.5.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Support for logical-system option introduced in Junos OS Release 13.3.

**Description**

Displays the status of BGP state replication between the master and backup Routing Engines on devices that have nonstop active routing configured on them.

---

**CAUTION:** Before attempting nonstop active routing switchover, check the output of show bgp replication to confirm that BGP routing table synchronization has completed on the backup Routing Engine. The complete status in the output of show task replication only indicates that the socket replication has completed and the BGP synchronization is in progress.

To determine whether BGP synchronization is complete, you must check the Protocol state and Synchronization state fields in the output of show bgp replication on the master Routing Engine. The Protocol state must be idle and the Synchronization state must be complete. If you perform NSR switchover before the BGP synchronization has completed, the BGP session might flap.

**Options**

This command has no options.

**Required Privilege Level**

view

**Related Documentation**

- show bgp replication logical-system

**List of Sample Output**

show bgp replication (for Master) on page 1770  
show bgp replication (for Backup) on page 1770

**Output Fields**

Table 66 on page 1769 lists the output fields for the show bgp replication command. Output fields are listed in the approximate order in which they appear.
Table 66: show bgp replication Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Precision timer registration | State of BGP precision timer feature in the kernel.  
  • **Registered**—BGP registers with the precision-timer feature in the kernel for auto keepalive generation after switchover.  
  • **NotRegistered**—Keepalive format of BGP is not registered.  |
| session state            | State of the current internal BGP state replication session, Up or Down, and the duration for which the session has been in the indicated state.  |
| flaps                    | Total number of flaps that occurred.                                                                                                                |
| protocol state           | Current state of the protocol operation, Active, Connect, Idle, and the duration for which the protocol has been in the indicated state.  |
| synchronization state    | Synchronization state at the time of executing the command. The states can be:  
  • **Idle**  
  • **Neighbor**—Indicates that the neighbor state synchronization is in progress.  
  • **AckWait**—Indicates that the request processing is over.  
  • **ORF**—Indicates that the outbound routing filter synchronization is in progress.  
  • **RIB**—Indicates that the routing table synchronization is in progress.  
  • **Complete**  |
| number of peers waiting  | Total number of peers waiting for various messages:  
  • **AckWait**—Number of peers waiting for a connection establishment or completed acknowledgment messages.  
  • **SoWait**—Number of peers waiting for TCP socket-related operations.  
  • **Scheduled**—Number of peers being synchronized.  |
| messages sent            | Number of various types of messages that have been sent since internal replication session became active:  
  • **Open**—Number of Open messages sent.  
  • **Establish**—Number of connection establishment acknowledgment messages sent.  
  • **Update**—Number of update messages sent.  
  • **Error**—Number of error messages sent.  
  • **Complete**—Number of connection complete acknowledgment messages sent.  |
| messages received        | Total number of messages received:  
  • **Open**—Number of Open messages received.  
  • **Request**—Number of request messages received:  
    • **Wildcard**—Number of requests received that used wildcards in the target address.  
    • **Targeted**—Number of requests received that used a specific address.  
  • **EstablishAck**—Number of connection establishment acknowledgement messages received.  
  • **CompleteAck**—Number of connection completed acknowledgement messages received.  |
Sample Output

show bgp replication (for Master)

user@host> show bgp replication

Synchronization master:
  Precision timer registration: Registered
  Session state: Up, Since: 10:14
  Flaps: 1, Last flap reason: Backup closed connection
  Protocol state: Idle, Since: 10:14
  Synchronization state: Complete
  Number of peers waiting: AckWait: 0, SoWait: 0, Scheduled: 0
  Messages sent: Open 1, Establish 11, GrHelper 0, Update 0, GrStaleLabel 0 Error 0, Complete 1
  Messages received: Open 1, Request 1 wildcard 0 targeted, EstablishAck 11, GrHelperAck 0, CompleteAck 1

show bgp replication (for Backup)

user@host> show bgp replication

Synchronization backup:
  State: Established 13 ago
  , Unsynchronized timer: 2

  Unsynchronized entry queue:
    Instance: 0 Neighbor: 30.30.30.1 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.3 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.4 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.5 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.6 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.1 elapsed: 7
    Instance: 0 Neighbor: 40.40.40.2 elapsed: 7
show bgp summary

List of Syntax  Syntax on page 1771
Syntax (EX Series Switch and QFX Series) on page 1771

Syntax  show bgp summary
<exact-instance instance-name>
<group group-name>
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and QFX Series)  show bgp summary
<instance instance-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
exact-instance option introduced in Junos OS Release 11.4.
group option introduced in Junos OS Release 13.3.

Description  Display BGP summary information.

Options  none—Display BGP summary information for all routing instances.

exact-instance instance-name—(Optional) Display information for the specified instance only.

group—Display overview of bgp information for a particular group

instance instance-name—(Optional) Display information for all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the show bgp summary instance cust1 command). The instance name can be master for the main instance, or any valid configured instance name or its prefix.

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 bgp summary (When a Peer Is Not Established) on page 1774
show bgp summary (When a Peer Is Established) on page 1774
show bgp summary (CLNS) on page 1774
show bgp summary (Layer 2 VPN) on page 1775
show bgp summary (Layer 3 VPN) on page 1775
show bgp summary group on page 1775
show bgp summary (BGP Graceful Restart or Long-Lived Graceful Restart) on page 1776

Output Fields

Table 67 on page 1772 describes the output fields for the show bgp summary command. Output fields are listed in the approximate order in which they appear.

Table 67: show bgp summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Number of BGP groups.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of BGP peers.</td>
</tr>
<tr>
<td>Down peers</td>
<td>Number of down BGP peers.</td>
</tr>
<tr>
<td>Table</td>
<td>Name of routing table.</td>
</tr>
<tr>
<td>Tot Paths</td>
<td>Total number of paths.</td>
</tr>
<tr>
<td>Act Paths</td>
<td>Number of active routes.</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Number of routes currently inactive because of damping or other reasons. These</td>
</tr>
<tr>
<td></td>
<td>routes do not appear in the forwarding table and are not exported by routing</td>
</tr>
<tr>
<td></td>
<td>protocols.</td>
</tr>
<tr>
<td>History</td>
<td>Number of withdrawn routes stored locally to keep track of damping history.</td>
</tr>
<tr>
<td>Damp State</td>
<td>Number of routes with a figure of merit greater than zero, but still active</td>
</tr>
<tr>
<td></td>
<td>because the value has not reached the threshold at which suppression occurs.</td>
</tr>
<tr>
<td>Pending</td>
<td>Routes in process by BGP import policy.</td>
</tr>
<tr>
<td>Peer</td>
<td>Address of each BGP peer. Each peer has one line of output.</td>
</tr>
<tr>
<td>AS</td>
<td>Peer’s AS number.</td>
</tr>
<tr>
<td>InPkt</td>
<td>Number of packets received from the peer.</td>
</tr>
<tr>
<td>OutPkt</td>
<td>Number of packets sent to the peer.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of BGP packets that are queued to be transmitted to a particular neighbor.</td>
</tr>
<tr>
<td></td>
<td>It normally is 0 because the queue usually is emptied quickly.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the BGP session has gone down and then come back up.</td>
</tr>
<tr>
<td>Last Up/Down</td>
<td>Last time since the neighbor transitioned to or from the established state.</td>
</tr>
</tbody>
</table>
Table 67: `show bgp summary` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State/Active/Received/Accepted/Damped</td>
<td>Multipurpose field that displays information about BGP peer sessions. The field's contents depend upon whether a session is established and whether it was established on the main routing device or in a routing instance.</td>
</tr>
<tr>
<td>• If a peer is not established, the field shows the state of the peer session: <strong>Active</strong>, <strong>Connect</strong>, or <strong>Idle</strong>. In general, the Idle state is the first stage of a connection. BGP is waiting for a Start event. A session can be idle for other reasons as well. The reason that a session is idle is sometimes displayed. For example: <strong>Idle (Removal in progress)</strong> or <strong>Idle (LicenseFailure)</strong>.</td>
<td></td>
</tr>
<tr>
<td>• If a BGP session is established on the main routing device, the field shows the number of active, received, accepted, and damped routes that are received from a neighbor and appear in the <em>inet.0</em> (main) and <em>inet.2</em> (multicast) routing tables. For example, <strong>8/10/10/2 and 2/4/4/0</strong> indicate the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8 active routes, 10 received routes, 10 accepted routes, and 2 damped routes from a BGP peer appear in the <em>inet.0</em> routing table.</td>
</tr>
<tr>
<td></td>
<td>• 2 active routes, 4 received routes, 4 accepted routes, and no damped routes from a BGP peer appear in the <em>inet.2</em> routing table.</td>
</tr>
<tr>
<td>• If a BGP session is established in a routing instance, the field indicates the established (<strong>Establ</strong>) state, identifies the specific routing table that receives BGP updates, and shows the number of active, received, and damped routes that are received from a neighbor. For example, <strong>Establ VPN-AB.inet.0: 2/4/0</strong> indicates the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The BGP session is established.</td>
</tr>
<tr>
<td></td>
<td>• Routes are received in the <strong>VPN-AB.inet.0</strong> routing table.</td>
</tr>
<tr>
<td></td>
<td>• The local routing device has two active routes, four received routes, and no damped routes from a BGP peer.</td>
</tr>
<tr>
<td></td>
<td>When a BGP session is established, the peers are exchanging update messages.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>When graceful restart or LLGR helper mode is active, the RIB information is now displayed by the <code>show bgp summary</code> command. If a BGP session is established on the main routing device, the field shows the number of active, received, accepted, and damped routes that are received from a neighbor and appear in the <em>inet.0</em> (main) and <em>inet.2</em> (multicast) routing tables. For example, <strong>8/10/10/2 and 2/4/4/0</strong> indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• 8 active routes, 10 received routes, 10 accepted routes, and 2 damped routes from a BGP peer appear in the <em>inet.0</em> routing table.</td>
</tr>
<tr>
<td></td>
<td>• 2 active routes, 4 received routes, 4 accepted routes, and no damped routes from a BGP peer appear in the <em>inet.2</em> routing table.</td>
</tr>
</tbody>
</table>
Sample Output

**show bgp summary (When a Peer Is Not Established)**

```
user@host> show bgp summary
Groups: 2 Peers: 4 Down peers: 1
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
----- |-----------|-----------|------------|---------|------|-------|-------
inet.0 | 6 | 4 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
----- |------|-------|--------|-----|-------|-----------
10.0.0.3 | 65002 | 86 | 90 | 0 | 2 | 42:54 0/0/0
10.0.0.4 | 65002 | 90 | 91 | 0 | 1 | 42:54 0/2/0
10.0.6 | 65002 | 87 | 90 | 0 | 3 | 3 Active
10.1.12.1 | 65001 | 89 | 89 | 0 | 1 | 42:54 4/4/0
0/0/0
```

**show bgp summary (When a Peer Is Established)**

```
user@host> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
----- |-----------|-----------|------------|---------|------|-------|-------
inet.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
----- |------|-------|--------|-----|-------|-----------
10.12.78.2 | 64531 | 27 | 26 | 0 | 0 | 10:49 Establ
inet.0 | 0/0/0/0
```

**show bgp summary logical-system R3**

```
user@host> show bgp summary logical-system R3
Groups: 2 Peers: 2 Down peers: 0
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
----- |-----------|-----------|------------|---------|------|-------|-------
bgp.l3vpn.0 | 2 | 2 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
----- |------|-------|--------|-----|-------|-----------
1.1.1.2 | 2 | 204 | 206 | 0 | 0 | 1:30:59 Establ
bgp.l3vpn.0: 2/2/2/0
red.inet.0: 2/2/2/0
10.1.1.10 | 3 | 206 | 207 | 0 | 0 | 1:31:36 Establ
red.inet.0: 2/2/2/0
```

**show bgp summary (CLNS)**

```
user@host> show bgp summary
Groups: 1 Peers: 1 Down peers: 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
----- |------|-------|--------|-----|-------|-----------
```

Copyright © 2019, Juniper Networks, Inc.
show bgp summary (Layer 2 VPN)

```
show bgp summary

Groups: 1 Peers: 5 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
bgp.l2vpn.0            1          1          0          0          0          0
inet.0                 0          0          0          0          0          0

Peer               AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Received/Damped...
10.255.245.35   65299         72         74       0       1       19:00 Establ
bgp.l2vpn.0: 1/1/0
frame-vpn.l2vpn.0: 1/1/0
10.255.245.36   65299       2164       2423       0       4       19:50 Establ
bgp.l2vpn.0: 0/0/0
frame-vpn.l2vpn.0: 0/0/0
10.255.245.37   65299         36         37       0       4       17:07 Establ
inet.0: 0/0/0
10.255.245.39   65299        138        168       0       6       53:48 Establ
bgp.l2vpn.0: 0/0/0
frame-vpn.l2vpn.0: 0/0/0
10.255.245.69   65299        134        140       0       6       53:42 Establ
inet.0: 0/0/0
```
### show bgp summary (BGP Graceful Restart or Long-Lived Graceful Restart)

```
user@router> show route-protocol bgp 10.4.12.11 detail
```

<table>
<thead>
<tr>
<th>Peer</th>
<th>AS</th>
<th>InPkt</th>
<th>OutPkt</th>
<th>OutQ</th>
<th>Flaps</th>
<th>Last Up/Dwn</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.255.16</td>
<td>100</td>
<td>7</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

```
bgp.l3vpn.0: 0/7/7/0
don- inet.0: 0/7/7/0
```

---

<table>
<thead>
<tr>
<th>Groups: 2 Peers: 2 Down peers: 0</th>
<th>Table</th>
<th>Tot Paths</th>
<th>Act Paths</th>
<th>Suppressed</th>
<th>History Damp State</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp.l3vpn.0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Peer State</td>
<td>InPkt</td>
<td>OutPkt</td>
<td>OutQ</td>
<td>Flaps</td>
<td>Last Up/Dwn</td>
<td></td>
</tr>
<tr>
<td>10.1.1.10</td>
<td>3</td>
<td>207</td>
<td>0</td>
<td>0</td>
<td>1:31:40</td>
<td></td>
</tr>
</tbody>
</table>

```
red.inet.0: 2/2/0
```
**show policy damping**

**List of Syntax**
- Syntax on page 1777
- Syntax (EX Series Switch and QFX Series) on page 1777

**Syntax**
```
show policy damping
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and QFX Series)**
```
show policy damping
```

**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 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display information about BGP route flap damping parameters.

**Options**
- none—Display information about BGP route flap damping parameters.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**
In the output from this command, figure-of-merit values correlate with the probability of future instability of a routing device. Routes with higher figure-of-merit values are suppressed for longer periods of time. The figure-of-merit value decays exponentially over time. A figure-of-merit value of zero is assigned to each new route. The value is increased each time the route is withdrawn or readvertised, or when one of its path attributes changes.

**Required Privilege Level**
- view

**Related Documentation**
- “Configuring BGP Flap Damping Parameters” in the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*
- clear bgp damping on page 1730
- show route damping on page 2299

**List of Sample Output**
- show policy damping on page 1778

**Output Fields**
- Table 68 on page 1778 describes the output fields for the `show policy damping` command. Output fields are listed in the approximate order in which they appear.
Table 68: show policy damping Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Halflife</td>
<td>Decay half-life, in minutes. The value represents the period during which the accumulated figure-of-merit value is reduced by half if the route remains stable. If a route has flapped, but then becomes stable, the figure-of-merit value for the route decays exponentially. For example, for a route with a figure-of-merit value of 1500, if no incidents occur, its figure-of-merit value is reduced to 750 after 15 minutes and to 375 after another 15 minutes.</td>
</tr>
<tr>
<td>Reuse merit</td>
<td>Figure-of-merit value below which a suppressed route can be used again. A suppressed route becomes reusable when its figure-of-merit value decays to a value below a reuse threshold, and the route once again is considered usable and can be installed in the forwarding table and exported from the routing table.</td>
</tr>
<tr>
<td>Suppress/cutoff merit</td>
<td>Figure-of-merit value above which a route is suppressed for use or inclusion in advertisements. When a route's figure-of-merit value reaches a particular level, called the cutoff or suppression threshold, the route is suppressed. When a route is suppressed, the routing table no longer installs the route into the forwarding table and no longer exports this route to any of the routing protocols.</td>
</tr>
<tr>
<td>Maximum suppress time</td>
<td>Maximum hold-down time, in minutes. The value represents the maximum time that a route can be suppressed no matter how unstable it has been before this period of stability.</td>
</tr>
<tr>
<td>Computed values</td>
<td>• Merit ceiling—Maximum merit that a flapping route can collect.</td>
</tr>
<tr>
<td></td>
<td>• Maximum decay—Maximum decay half-life, in minutes.</td>
</tr>
</tbody>
</table>

Sample Output

show policy damping

user@host> show policy damping

Default damping information:
  Halflife: 15 minutes
  Reuse merit: 750 Suppress/cutoff merit: 3000
  Maximum suppress time: 60 minutes
  Computed values:
    Merit ceiling: 12110
    Maximum decay: 6193

Damping information for "standard-damping":
  Halflife: 10 minutes
  Reuse merit: 4000 Suppress/cutoff merit: 8000
  Maximum suppress time: 30 minutes
  Computed values:
    Merit ceiling: 32120
    Maximum decay: 12453
CHAPTER 18

ES-IS Operational Commands

- clear esis adjacency
- clear esis statistics
- show esis adjacency
- show esis interface
- show esis statistics
clear esis adjacency

Syntax

```
clear esis adjacency
<instance instance-name>
<interface interface-name>
<neighbor>
```

Release Information
Command introduced before Junos OS Release 7.4.

Description

Options
- **none**—Clear all ES-IS adjacencies.
- **instance instance-name**—(Optional) Clear adjacencies for the specified routing instance only.
- **interface interface-name**—(Optional) Clear adjacencies for the specified interface only.
- **neighbor**—(Optional) Clear adjacencies for the specified neighbor only.

Required Privilege
- **clear**

Related Documentation
- [show esis adjacency on page 1782](#)

List of Sample Output
- [clear esis adjacency on page 1780](#)

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear esis adjacency

user@host> clear esis adjacency
```
clear esis statistics

Syntax

```
clear esis statistics
<instance instance-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description


Options

- none—Clear ES-IS packet statistics for all routing instances.
- instance instance-name—(Optional) Clear ES-IS packet statistics for the specified routing instance only.

Required Privilege

```
clear
```

Related Documentation

- show esis statistics on page 1787

List of Sample Output

```
clear esis statistics on page 1781
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear esis statistics
```

```
user@host> clear esis statistics
```
show esis adjacency

**Syntax**

```
show esis adjacency
<brief | detail | extensive>
<esis-neighbor-id>
<instance instance-name>
<interface interface-name>)
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Display End System-to-Intermediate System (ES-IS) adjacencies.

**Options**

- **none**—(Same as **brief**) Display all ES-IS adjacencies.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **esis-neighbor-id**—(Optional) Display adjacencies for the specified neighbor's network service access point (NSAP) only.
- **instance instance-name**—(Optional) Display adjacencies for the specified routing instance only.
- **interface interface-name**—(Optional) Display adjacencies for the specified interface only.

**Required Privilege**

- **Level**

  - **view**

**Related Documentation**

- **clear esis adjacency on page 1780**

**List of Sample Output**

- **show esis adjacency on page 1783**
- **show esis adjacency brief on page 1783**
- **show esis adjacency detail on page 1783**
- **show esis adjacency extensive on page 1783**

**Output Fields**

Table 69 on page 1782 describes the output fields for the **show esis adjacency** 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><strong>Nbr Type</strong></td>
<td>Type of network service access point (NSAP) of this neighbor.</td>
<td><strong>brief</strong> none</td>
</tr>
<tr>
<td><strong>NSAP/NET</strong></td>
<td>NSAP of this neighbor.</td>
<td><strong>All levels</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of NSAP of this neighbor.</td>
<td><strong>detail extensive</strong></td>
</tr>
</tbody>
</table>
Table 69: show esis adjacency Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold (secs)</td>
<td>Holdtime interval advertised by this neighbor.</td>
<td>brief none</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Advertised holdtime</td>
<td>Holdtime interval advertised by this neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Expires in</td>
<td>How long until the adjacency expires, in seconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the neighbor).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transition log</td>
<td>List of recent transitions.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• When—Time of advertisement from this neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of the adjacency: Up, Down, New, One-way, Initializing, or Rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event—Event causing the state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down reason—Reason the adjacency is down.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

**show esis adjacency**

```
user@host> show esis adjacency
```

<table>
<thead>
<tr>
<th>Nbr</th>
<th>NSAP/NET</th>
<th>Hold (secs)</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS</td>
<td>47.0005.80ff.f800.0000.0108.0001.0102.5501.6008</td>
<td>135</td>
<td>fe-0/0/0.0</td>
</tr>
</tbody>
</table>

**show esis adjacency brief**

The output for the `show esis adjacency brief` command is identical to that for the `show esis adjacency` command. For sample output, see `show esis adjacency` on page 1783.

**show esis adjacency detail**

```
user@host> show esis adjacency detail
```

NSAP/NET: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6008, Type: IS
Interface: fe-0/0/0.0, Advertised hold time: 180 secs, Expires in: 173 secs
SNPA: 0:5:85:c1:73:71

**show esis adjacency extensive**

```
user@host> show esis adjacency extensive
```

NSAP/NET: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6008, Type: IS
Interface: fe-0/0/0.0, Advertised hold time: 180 secs, Expires in: 167 secs
SNPA: 0:5:85:c1:73:71
Transition log:
<table>
<thead>
<tr>
<th>When</th>
<th>State</th>
<th>Event</th>
<th>Down reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Nov 26 22:07:35</td>
<td>Up</td>
<td>Received ISH</td>
<td></td>
</tr>
</tbody>
</table>
show esis interface

Syntax

```
show esis interface
  <brief | detail | extensive>
  <instance instance-name>
  <interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description


Options

- `none`—(Same as `brief`) Display information for all configured ES-IS interfaces.
- `brief | detail | extensive`—(Optional) Display the specified level of output.
- `instance instance-name`—(Optional) Display configured interfaces for the specified routing instance only.
- `interface interface-name`—(Optional) Display information about the specified interface only.

Required Privilege

`view`

List of Sample Output

- `show esis interface on page 1786`
- `show esis interface brief on page 1786`
- `show esis interface detail on page 1786`
- `show esis interface extensive on page 1786`

Output Fields

Table 70 on page 1785 describes the output fields for the `show esis interface` command. Output fields are listed in the approximate order in which they appear.

### Table 70: show esis 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 through which the adjacency is made.</td>
<td>All levels</td>
</tr>
<tr>
<td>Receives</td>
<td>Types of hello messages that are received.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sends</td>
<td>Types of hello messages that are sent.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hello interval</td>
<td>Interface's hello interval, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Adjacencies or Num Adj</td>
<td>Number of adjacencies established on this interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Interface's hold time, in seconds.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 70: show esis 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>State</td>
<td>Internal implementation information.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>End system configuration timer</td>
<td>Time, in seconds, for the end system to configure itself for ES-IS.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index value.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>NET used in hello</td>
<td>Network entity title used in hello messages.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show esis interface

user@host> show esis interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Receives</th>
<th>Sends</th>
<th>Hello Interval</th>
<th>Num Adj</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/0.0</td>
<td>ISH</td>
<td>ISH</td>
<td>60.00</td>
<td>1</td>
</tr>
<tr>
<td>lo0.0</td>
<td>ISH</td>
<td>-</td>
<td>60.00</td>
<td>0</td>
</tr>
</tbody>
</table>

show esis interface brief

The output for the show esis interface brief command is identical to that for the show esis interface command. For sample output, see show esis interface on page 1786.

show esis interface detail

user@host> show esis interface detail

Interface: fe-0/0/0.0
  Receives: ISH, Sends: ISH, Hello interval: 60.00
  Adjacencies: 1, Holdtime: 180, End system configuration timer: 180
  Interface index: 68, State: 0x2
  NET used in hello: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6007

Interface: lo0.0
  Receives: ISH, Sends: - , Hello interval: 60.00
  Adjacencies: 0, Holdtime: 180, End system configuration timer: 180
  Interface index: 64, State: 0x2
  NET used in hello: 47.0005.80ff.f800.0000.0108.0001.0102.5501.6007

show esis interface extensive

The output for the show esis interface extensive command is identical to that for the show esis interface detail command. For sample output, see show esis interface detail on page 1786.
**show esis statistics**

**Syntax**  
show esis statistics  
<instance instance-name>

**Release Information**  
Command introduced before Junos OS Release 7.4.

**Description**  

**Options**  
- **none**—Display ES-IS packet statistics for all routing instances.
- **instance instance-name**—(Optional) Display ES-IS statistics for the specified routing instance only.

**Required Privilege**  
view

**Related Documentation**  
- clear esis statistics on page 1781
- show esis statistics on page 1788

**List of Sample Output**  
show esis statistics on page 1788

**Output Fields**  
Table 71 on page 1787 describes the output fields for the show esis statistics 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>PDU type</td>
<td>Protocol data unit type.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of PDUs received since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>Processed</td>
<td>Number of PDUs received less the number dropped.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of PDUs dropped.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of PDUs transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>Total packets received/sent</td>
<td>Total number of PDUs received and transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
</tbody>
</table>
## Sample Output

`show esis statistics`

```
user@host> show esis statistics

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESH</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>ISH</td>
<td>11</td>
<td>10</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>RD</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>14</td>
<td>13</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>

Total packets received: 14 sent: 0
```
CHAPTER 19

IP Multicast Operational Commands

- clear amt statistics
- clear amt tunnel
- clear igmp membership
- clear igmp snooping membership
- clear igmp snooping statistics
- clear igmp statistics
- clear mld membership
- clear mld statistics
- clear msdp cache
- clear msdp statistics
- clear multicast bandwidth-admission
- clear multicast forwarding-cache
- clear multicast scope
- clear multicast sessions
- clear multicast snooping statistics
- clear multicast statistics
- clear pim join
- clear pim join-distribution
- clear pim register
- clear pim snooping join
- clear pim snooping statistics
- clear pim statistics
- request pim multicast-tunnel rebalance
- show amt statistics
- show amt summary
- show amt tunnel
- show dvmrp interfaces
- show dvmrp neighbors
• show dvmrp prefix
• show dvmrp prunes
• show igmp group
• show igmp interface
• show igmp snooping interface
• show igmp snooping membership
• show igmp snooping statistics
• show igmp statistics
• show mld group
• show mld interface
• show mld statistics
• show msdp
• show msdp source
• show msdp source-active
• show msdp statistics
• show multicast backup-pe-groups
• show multicast flow-map
• show multicast forwarding-cache statistics
• show multicast interface
• show multicast mrinfo
• show multicast next-hops
• show multicast pim-to-igmp-proxy
• show multicast pim-to-mld-proxy
• show multicast route
• show multicast rpf
• show multicast scope
• show multicast snooping next-hops
• show multicast sessions
• show multicast snooping route
• show multicast statistics
• show multicast usage
• show pim bootstrap
• show pim interfaces
• show pim join
• show pim mdt
• show pim mdt data-mdt-joins
• show pim mdt data-mdt-limit
- `show pim neighbors`
- `show pim rps`
- `show pim snooping interfaces`
- `show pim snooping join`
- `show pim snooping neighbors`
- `show pim snooping statistics`
- `show pim source`
- `show pim statistics`
- `show sap listen`
- `test msdp`
clear amt statistics

**Syntax**

```
clear amt statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced in JUNOS Release 10.2.

**Description**

Clear Automatic Multicast Tunneling (AMT) statistics.

**Options**

- **none**—Clear the multicast statistics for all AMT tunnel interfaces.
- **instance instance-name**—(Optional) Clear AMT multicast statistics for the specified instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

clear

**Related Documentation**

- show amt statistics on page 1830

**List of Sample Output**

- clear amt statistics on page 1792

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear amt statistics

user@host> clear amt statistics
```
clear amt tunnel

Syntax  

```plaintext
<gateway gateway-ip-addr> <port port-number>
<instance instance-name>
<logical-system (all | logical-system-name)>
<statistics>
<tunnel-interface interface-name>
```

Release Information  
Command introduced in JUNOS Release 10.2.

Description  
Clear the Automatic Multicast Tunneling (AMT) multicast state. Optionally, clear AMT protocol statistics.

Options  

- **none**—Clear multicast state for all AMT tunnel interfaces.

- **gateway gateway-ip-addr port port-number**—(Optional) Clear the AMT multicast state for the specified gateway address. If no port is specified, clear the AMT multicast state for all AMT gateways with the given IP address.

- **instance instance-name**—(Optional) Clear the AMT multicast state for the specified instance.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

- **statistics**—(Optional) Clear multicast statistics for all AMT tunnels or for specified tunnels.

- **tunnel-interface interface-name**—(Optional) Clear the AMT multicast state for the specified AMT tunnel interface.

Required Privilege  
Level clear

Related Documentation  
- show amt tunnel on page 1835

List of Sample Output  

- clear amt tunnel on page 1793

- clear amt tunnel statistics gateway-address on page 1794

Output Fields  
When you enter this command, you are provided feedback on the status of your request.

Sample Output  

clear amt tunnel

```
user@host> clear amt tunnel
```
clear amt tunnel statistics gateway-address

user@host> clear amt tunnel statistics gateway-address 100.31.21 port 4000
clear igmp membership

List of Syntax  Syntax on page 1795
Syntax (EX Series Switch and the QFX Series) on page 1795

Syntax

```
clear igmp membership
<all>
<group address-range>
<integer interface-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
clear igmp membership
<group address-range>
<integer interface-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Clear Internet Group Management Protocol (IGMP) group members.

Options

```
all—Clear IGMP members for groups and interfaces in the master instance.

<group address-range>—(Optional) Clear all IGMP members that are in a particular address range. An example of a range is 233.252/16. If you omit the destination prefix length, the default is /32.

<integer interface-name>—(Optional) Clear all IGMP group members on an interface.

<logical-system (all | logical-system-name)>—(Optional) Perform this operation on all logical systems or on a particular logical system.
```

Required Privilege

```
clear
```

Level

Related Documentation

```
• show igmp group on page 1849
• show igmp interface on page 1853
```

List of Sample Output

```
clear igmp membership all on page 1796
clear igmp membership interface on page 1796
clear igmp membership group on page 1797
```

Output Fields

See show igmp group for an explanation of output fields.
Sample Output

clear igmp membership all

The following sample output displays IGMP group information before and after the `clear igmp membership` command is entered:

```
user@host> show igmp group

Interface        Group           Last Reported   Timeout
so-0/0/0         198.51.100.253   203.0.113.1          186
so-0/0/0         198.51.100.254   203.0.113.1          186
so-0/0/0         198.51.100.255   203.0.113.1          187
so-0/0/0         198.51.100.240   203.0.113.1          188
local            198.51.100.6     (null)                0
local            198.51.100.5     (null)                0
local            198.51.100.254   (null)                0
local            198.51.100.255   (null)                0
local            198.51.100.2     (null)                0
local            198.51.100.13    (null)                0

user@host> clear igmp membership all

Clearing Group Membership Info for so-0/0/0
Clearing Group Membership Info for so-1/0/0
Clearing Group Membership Info for so-2/0/0

user@host> show igmp group

Interface        Group           Last Reported   Timeout
local            198.51.100.6     (null)                0
local            198.51.100.5     (null)                0
local            198.51.100.254   (null)                0
local            198.51.100.255   (null)                0
local            198.51.100.2     (null)                0
local            198.51.100.13    (null)                0
```

clear igmp membership interface

The following sample output displays IGMP group information before and after the `clear igmp membership interface` command is issued:

```
user@host> show igmp group

Interface        Group           Last Reported   Timeout
so-0/0/0         198.51.100.253   203.0.113.1          210
so-0/0/0         198.51.100.200   203.0.113.1          210
so-0/0/0         198.51.100.255   203.0.113.1          215
so-0/0/0         198.51.100.240   203.0.113.1          216
local            198.51.100.6     (null)                0
local            198.51.100.5     (null)                0
local            198.51.100.254   (null)                0
local            198.51.100.255   (null)                0
local            198.51.100.2     (null)                0
local            198.51.100.13    (null)                0

user@host> clear igmp membership interface so-0/0/0
```
Clearing Group Membership Info for so-0/0/0

user@host> show igmp group

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Last Reported</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>198.51.100.6</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.5</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.254</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.255</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.2</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.13</td>
<td>(null)</td>
<td>0</td>
</tr>
</tbody>
</table>

clear igmp membership group

The following sample output displays IGMP group information before and after the clear igmp membership group command is entered:

user@host> show igmp group

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Last Reported</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.253</td>
<td>203.0.113.1</td>
<td>210</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.25</td>
<td>203.0.113.1</td>
<td>210</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.255</td>
<td>203.0.113.1</td>
<td>215</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.254</td>
<td>203.0.113.1</td>
<td>216</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.6</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.5</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.254</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.255</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.2</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.13</td>
<td>(null)</td>
<td>0</td>
</tr>
</tbody>
</table>

user@host> clear igmp membership group 233.252/16

Clearing Group Membership Range 198.51.100.0/16 on so-0/0/0
Clearing Group Membership Range 198.51.100.0/16 on so-1/0/0
Clearing Group Membership Range 198.51.100.0/16 on so-2/0/0

user@host> show igmp group

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Last Reported</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.255</td>
<td>203.0.113.1</td>
<td>231</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.254</td>
<td>203.0.113.1</td>
<td>233</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>198.51.100.253</td>
<td>203.0.113.1</td>
<td>236</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.6</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.5</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.254</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.255</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.2</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>198.51.100.13</td>
<td>(null)</td>
<td>0</td>
</tr>
</tbody>
</table>
clear igmp snooping membership

Syntax

```
clear igmp snooping membership
  <vlan vlan-name >
  <group | source address>
  <instance instance-name>
  <interface interface-name>
  <learning-domain learning-domain-name>
  <logical-system logical-system-name>
  <vlan-id vlan-identifier>
```

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 18.1R1 for the SRX1500 devices.

Description

Clear IGMP snooping dynamic membership information from the multicast forwarding table.

Options

none—Clear IGMP snooping membership for all supported address families on all interfaces.

`vlan vlan-name`—(Optional) Clear dynamic membership information for the specified VLAN.

`group | source address`—(Optional) Clear IGMP snooping membership for the specified multicast group or source address.

`instance instance-name`—(Optional) Clear IGMP snooping membership for the specified instance.

`interface interface-name`—(Optional) Clear IGMP snooping membership on a specific interface.

`learning-domain learning-domain-name`—(Optional) Perform this operation on all learning domains or on a particular learning domain.

`logical-system logical-system-name`—(Optional) Display information about a particular logical system, or for all logical systems.

`vlan-id vlan-identifier`—(Optional) Perform this operation on a particular VLAN.

Required Privilege Level
clear

Related Documentation

- show igmp snooping membership on page 1863

List of Sample Output
clear igmp snooping membership on page 1799

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear igmp snooping membership

user@host> clear igmp snooping membership
clear igmp snooping statistics

Syntax

```
clear igmp snooping statistics
<instance instance-name>
<interface interface-name>
<learning-domain (all | learning-domain-name)>
<logical-system logical-system-name>
```

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 18.1R1 for the SRX1500 devices.

Description

Clear IP IGMP snooping statistics.

Options

- `none`—Clear IGMP snooping statistics for all supported address families on all interfaces.
- `instance instance-name`—(Optional) Clear IGMP snooping statistics for the specified instance.
- `interface interface-name`—(Optional) Clear IGMP snooping statistics on a specific interface.
- `learning-domain (all | learning-domain-name)`—(Optional) Perform this operation on all learning domains or on a particular learning domain.
- `logical-system logical-system-name`—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.

Required Privilege Level

clear

Related Documentation

- show igmp snooping statistics on page 1869

List of Sample Output

- clear igmp snooping statistics on page 1800

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear igmp snooping statistics

```
user@host> clear igmp snooping statistics
```
clear igmp statistics

**List of Syntax**
- Syntax on page 1801
- Syntax (EX Series Switches) on page 1801

**Syntax**
```
 clear igmp statistics
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
 clear igmp statistics
  <interface interface-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Clear Internet Group Management Protocol (IGMP) statistics.

**Options**
- none—Clear IGMP statistics on all interfaces.
- `interface` *interface-name*—(Optional) Clear IGMP statistics for the specified interface only.
- `logical-system` *(all | logical-system-name)*—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
clear

**Related Documentation**
- show igmp statistics on page 1874

**List of Sample Output**
clear igmp statistics on page 1801

**Output Fields**
See show igmp statistics for an explanation of output fields.

**Sample Output**
clear igmp statistics

The following sample output displays IGMP statistics information before and after the `clear igmp statistics` command is entered:

```
user@host> show igmp statistics
```

Copyright © 2019, Juniper Networks, Inc.
IGMP packet statistics for all interfaces

<table>
<thead>
<tr>
<th>IGMP Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Query</td>
<td>8883</td>
<td>459</td>
<td>0</td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP</td>
<td>19784</td>
<td>35476</td>
<td>0</td>
</tr>
<tr>
<td>PIM V1</td>
<td>18310</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Request</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 unsupported type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 source required for SSM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 mode not applicable for SSM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IGMP Global Statistics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>0</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>0</td>
</tr>
<tr>
<td>Rx non-local</td>
<td>1227</td>
</tr>
</tbody>
</table>
clear mld membership

Syntax

```
clear mld membership
<all>
<group group-name>
@interface interface-name>
logical-system (all | logical-system-name)>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear Multicast Listener Discovery (MLD) group membership.

Options

- **all**—Clear MLD memberships for groups and interfaces in the master instance.
- **group group-name**—(Optional) Clear MLD membership for the specified group.
- **interface interface-name**—(Optional) Clear MLD group membership for the specified interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

```
view
```

Related Documentation

- `show mld group` on page 1877

List of Sample Output

- clear mld membership all on page 1803

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear mld membership all

user@host> clear mld membership all
```
# clear mld statistics

**Syntax**

```plaintext
clear mld statistics
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Clear Multicast Listener Discovery (MLD) statistics.

**Options**

- `none`—(Same as `logical-system all`) Clear MLD statistics for all interfaces.
- `interface interface-name`—(Optional) Clear MLD statistics for the specified interface.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- `clear`

**Related Documentation**

- [show mld statistics on page 1885](#)

**List of Sample Output**

- clear mld statistics on page 1804

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```plaintext
user@host> clear mld statistics
```

---

Copyright © 2019, Juniper Networks, Inc.
**clear msdp cache**

**Syntax**

```
clear msdp cache
<all>
<instance instance-name>
<logical-system (all | logical-system-name)>
<peer peer-address>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Clear the entries in the Multicast Source Discovery Protocol (MSDP) source-active cache.

**Options**

- **all**—Clear all MSDP source-active cache entries in the master instance.
- **instance instance-name**—(Optional) Clear entries for a specific MSDP instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **peer peer-address**—(Optional) Clear the MSDP source-active cache entries learned from a specific peer.

**Required Privilege**

- **clear**

**Related Documentation**

- `show msdp source-active on page 1893`

**List of Sample Output**

- `clear msdp cache all on page 1805`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear msdp cache all

user@host> clear msdp cache all
```
clear msdp statistics

Syntax

clear msdp statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
<peer peer-address>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Clear Multicast Source Discovery Protocol (MSDP) peer statistics.

Options

none—Clear MSDP statistics for all peers.

instance instance-name—(Optional) Clear statistics for the specified instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

peer peer-address—(Optional) Clear the statistics for the specified peer.

Required Privilege
clear

Level

Related Documentation

• show msdp statistics on page 1896

List of Sample Output
clear msdp statistics on page 1806

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
clear msdp statistics

user@host> clear msdp statistics
clear multicast bandwidth-admission

Syntax

```
clear multicast bandwidth-admission
<group group-address>
/inet | inet6>
<instance instance-name>
<source source-address>
```

Release Information

- Command introduced in Junos OS Release 8.3.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Reapply IP multicast bandwidth admissions.

Options

- **none**—Reapply multicast bandwidth admissions for all IPv4 forwarding entries in the master routing instance.

- **group group-address**—(Optional) Reapply multicast bandwidth admissions for the specified group.

- **inet**—(Optional) Reapply multicast bandwidth admission settings for IPv4 flows.

- **inet6**—(Optional) Reapply multicast bandwidth admission settings for IPv6 flows.

- **instance instance-name**—(Optional) Reapply multicast bandwidth admission settings for the specified instance. If you do not specify an instance, the command applies to the master routing instance.

- **interface interface-name**—(Optional) Examines the corresponding outbound interface in the relevant entries and acts as follows:
  
  - If the interface is congested, and it was admitted previously, it is removed.
  - If the interface was rejected previously, the `clear multicast bandwidth-admission` command enables the interface to be admitted as long as enough bandwidth exists on the interface.
  - If you do not specify an interface, issuing the `clear multicast bandwidth-admission` command readmits any previously rejected interface for the relevant entries as long as enough bandwidth exists on the interface.

  To manually reject previously admitted outbound interfaces, you must specify the interface.

- **source source-address**—(Optional) Use with the `group` option to reapply multicast bandwidth admission settings for the specified (source, group) entry.
Required Privilege Level  clear

Related Documentation  •  show multicast interface on page 1906

List of Sample Output  clear multicast bandwidth-admission on page 1808

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output
clear multicast bandwidth-admission

user@host> clear multicast bandwidth-admission
clear multicast forwarding-cache

**Syntax**
clear multicast forwarding-cache
<all>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>

**Release Information**
Command introduced in Junos OS Release 12.2.

**Description**
Clear IP multicast forwarding cache entries.

This command is not supported for next-generation multiprotocol BGP multicast VPNs (MVPNs).

**Options**
- **all**—Clear all multicast forwarding cache entries in the master instance.
- **inet**—(Optional) Clear multicast forwarding cache entries for IPv4 family addresses.
- **inet6**—(Optional) Clear multicast forwarding cache entries for IPv6 family addresses.
- **instance instance-name**—(Optional) Clear multicast forwarding cache entries on a specific routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
clear

**Related Documentation**
- show multicast forwarding-cache statistics on page 1904

**List of Sample Output**
clear multicast forwarding-cache all on page 1809

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear multicast forwarding-cache all

user@host> clear multicast forwarding-cache all
clear multicast scope

List of Syntax
- Syntax on page 1810
- Syntax (EX Series Switch and the QFX Series) on page 1810

Syntax
```plaintext
clear multicast scope
<inet | inet6>
<interface interface-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)
```plaintext
clear multicast scope
<inet | inet6>
<interface interface-name>
```

Release Information
- Command introduced in Junos OS Release 7.6.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `inet6` option introduced in Junos OS Release 10.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Clear IP multicast scope statistics.

Options
- **none**—(Same as `logical-system all`) Clear multicast scope statistics.
- **inet**—(Optional) Clear multicast scope statistics for IPv4 family addresses.
- **inet6**—(Optional) Clear multicast scope statistics for IPv6 family addresses.
- **interface interface-name**—(Optional) Clear multicast scope statistics on a specific interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level
clear

Related Documentation
- show multicast scope on page 1934

List of Sample Output
clear multicast scope on page 1811

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear multicast scope

user@host> clear multicast scope
clear multicast sessions

List of Syntax  Syntax on page 1812
                  Syntax (EX Series Switch and the QFX Series) on page 1812

Syntax                  clear multicast sessions
                  <logical-system (all | logical-system-name)>
                  <regular-expression>

Syntax (EX Series Switch and the QFX Series)                  clear multicast sessions
                  <regular-expression>

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 11.3 for the QFX Series.
                  Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description                  Clear IP multicast sessions.

Options                  none—(Same as logical-system all) Clear multicast sessions.
                  logical-system (all | logical-system-name)—(Optional) Perform this operation on all
                  logical systems or on a particular logical system.
                  regular-expression—(Optional) Clear only multicast sessions that contain the specified
                  regular expression.

Required Privilege Level                  clear

Related Documentation                  •  show multicast sessions on page 1940

List of Sample Output                  clear multicast sessions on page 1812

Output Fields                  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear multicast sessions

user@host> clear multicast sessions
clear multicast snooping statistics

Syntax

```
clear multicast snooping statistics
  <instance instance-name>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

Release Information

Command introduced in Junos OS Release 8.5.

Description

Clear IP multicast snooping statistics.

Options

- **none**—Clear multicast snooping statistics for all supported address families on all interfaces.
- **instance instance-name**—(Optional) Clear multicast snooping statistics for the specified instance.
- **interface interface-name**—(Optional) Clear multicast snooping statistics on a specific interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

- **clear**

List of Sample Output

clear multicast snooping statistics on page 1813

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear multicast snooping statistics

```
user@host> clear multicast snooping statistics
```
clear multicast statistics

**List of Syntax**

Syntax on page 1814
Syntax (EX Series Switch and the QFX Series) on page 1814
Syntax (EX4300 Switch) on page 1814

**Syntax**
clear multicast statistics

- `<inet | inet6>`
- `<instance instance-name>`
- `<interface interface-name>`
- `<logical-system (all | logical-system-name)>`

**Syntax (EX Series Switch and the QFX Series)**
clear multicast statistics

- `<inet | inet6>`
- `<instance instance-name>`
- `<interface interface-name>`

**Syntax (EX4300 Switch)**
clear system-packet-forwarding-options multicast-statistics

There are no available options for the EX4300.

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Syntax added in Junos OS Release 19.2R1 for clearing multicast route statistics (EX4300 switches).

**Description**
Clear IP multicast statistics.

**Options**
- `none`—Clear multicast statistics for all supported address families on all interfaces.
- `inet`—(Optional) Clear multicast statistics for IPv4 family addresses.
- `inet6`—(Optional) Clear multicast statistics for IPv6 family addresses.
- `instance instance-name`—(Optional) Clear multicast statistics for the specified instance.
- `interface interface-name`—(Optional) Clear multicast statistics on a specific interface.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level
clear

Related Documentation
- show multicast statistics on page 1948

List of Sample Output
clear multicast statistics on page 1815

Output Fields
When you enter this command, you get feedback on the status of your request.

Sample Output
clear multicast statistics

user@host> clear multicast statistics
clear pim join

**List of Syntax**

Syntax (EX Series Switch and the QFX Series) on page 1816

```
Syntax clear pim join
<all>
<group-address>
<bidirectional | dense | sparse>
<exact>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
*inet6* and *instance* options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Multiple new filter options introduced in Junos OS Release 13.2.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Clear the Protocol Independent Multicast (PIM) join and prune states.

**Options**

*all*—To clear PIM join and prune states for all groups and family addresses in the master instance, you must specify “all”.

*group-address*—(Optional) Clear the PIM join and prune states for a group address.

*bidirectional | dense | sparse*—(Optional) Clear PIM bidirectional mode, dense mode, or sparse and source-specific multicast (SSM) mode entries.

*exact*—(Optional) Clear only the group that exactly matches the specified group address.

*inet | inet6*—(Optional) Clear the PIM entries for IPv4 or IPv6 family addresses, respectively.
instance instance-name—(Optional) Clear the entries for a specific PIM-enabled routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

rp ip-address/prefix | source ip-address/prefix—(Optional) Clear the PIM entries with a specified rendezvous point (RP) address and prefix or with a specified source address and prefix. You can omit the prefix.

sg | star-g—(Optional) Clear PIM (S,G) or (*,G) entries.

Additional Information
The clear pim join command cannot be used to clear the PIM join and prune state on a backup Routing Engine when nonstop active routing is enabled.

Required Privilege
Level
clear

Related Documentation
• show pim join on page 1961

List of Sample Output
clear pim join all on page 1817
clear pim join inet6 all on page 1817
clear pim join inet6 star-g all on page 1817

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear pim join all

user@host> clear pim join all
Cleared 8 Join/Prune states

clear pim join inet6 all

user@host> clear pim join inet6 all
Cleared 4 Join/Prune states

clear pim join inet6 star-g all

user@host> clear pim join inet6 star-g all
Cleared 1 Join/Prune states
clear pim join-distribution

Syntax

clear pim join-distribution
<all>
<instance instance-name>
<logical-system (all | logical-system-name)>

Release Information
Command introduced in Junos OS Release 10.0.

Description
Clear the PIM join-redistribute states.

Use the show pim source command to find out if there are multiple paths available for a source (for example, an RP).

When you include the join-load-balance statement in the configuration, the PIM join states are distributed evenly on available equal-cost multipath links. When an upstream neighbor link fails, Junos OS redistributes the PIM join states to the remaining links. However, when new links are added or the failed link is restored, the existing PIM joins are not redistributed to the new link. New flows will be distributed to the new links. However, in a network without new joins and prunes, the new link is not used for multicast traffic. The clear pim join-distribution command redistributes the existing flows to the new upstream neighbors. Redistributing the existing flows causes traffic to be disrupted, so we recommend that you run the clear pim join-distribution command during a maintenance window.

Options
all— (Optional) Clear the PIM join-redistribute states for all groups and family addresses in the master instance.

none— Automatically clear all PIM join/prune states.

instance instance-name— (Optional) Redistribute the join states for a specific PIM-enabled routing instance.

logical-system (all | logical-system-name)— (Optional) Perform this operation on all logical systems or on a particular logical system.

Additional Information
The clear pim join-distribution command cannot be used to redistribute the PIM join states on a backup Routing Engine when nonstop active routing is enabled.

Required Privilege
Level

clear

Related Documentation
• show pim neighbors on page 1985
• show pim join on page 1961
• join-load-balance
List of Sample Output  clear pim join-distribution all on page 1819

Output Fields  When you enter this command, you are provided no feedback on the status of your request. You can enter the show pim join command before and after distributing the join state to verify the operation.

Sample Output

clear pim join-distribution all

user@host> clear pim join-distribution all
clear pim register

List of Syntax
Syntax on page 1820
Syntax (EX Series Switch and the QFX Series) on page 1820
Syntax (PTX Series) on page 1820

Syntax clear pim register
<all>
<inet | inet6>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series) clear pim register
<inet | inet6>
<instance instance-name>
<interface interface-name>

Syntax (PTX Series) clear pim register
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>

Release Information
Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Clear Protocol Independent Multicast (PIM) register message counters.

Options
all—Required to clear the PIM register message counters for all groups and family addresses in the master instance.

inet | inet6—(Optional) Clear PIM register message counters for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Clear register message counters for a specific PIM-enabled routing instance.

interface interface-name—(Optional) Clear PIM register message counters for a specific interface.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Additional Information: The `clear pim register` command cannot be used to clear the PIM register state on a backup Routing Engine when nonstop active routing is enabled.

Required Privilege Level: clear

Related Documentation: • show pim statistics on page 2018

List of Sample Output: `clear pim register all` on page 1821

Output Fields: When you enter this command, you are provided feedback on the status of your request.

Sample Output:
```
clear pim register all

user@host> clear pim register all
```
clear pim snooping join

Syntax

```
clear pim snooping join
<instance instance-name>
logical-system logical-system-name
<vlan-id vlan-id>
```

Release Information

Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

Description

Clear information about Protocol Independent Multicast (PIM) snooping joins.

Options

- `none`—Display detailed information.
- `instance instance-name`—(Optional) Clear PIM snooping join information for the specified routing instance.
- `logical-system logical-system-name`—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.
- `vlan-id vlan-identifier`—(Optional) Clear PIM snooping join information for the specified VLAN.

Required Privilege

- `view`

Related Documentation

- [PIM Snooping for VPLS](#)

List of Sample Output

clear pim snooping join on page 1822

Output Fields

See [show pim snooping join](#) for an explanation of the output fields.

Sample Output

clear pim snooping join

The following sample output displays information about PIM snooping joins before and after the `clear pim snooping join` command is entered:

```
user@host> show pim snooping join extensive

Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

Group: 198.51.100.2
Source: *
```
| Flags: sparse,rptree,wildcard |
| Upstream state: None         |
| Upstream neighbor: 192.0.2.5, port: ge-1/3/7.20 |
| Downstream port: ge-1/3/1.20 |
| Downstream neighbors:       |
| 192.0.2.2 State: Join Flags: SRW Timeout: 185 |

| Group: 198.51.100.3 |
| Source: * |
| Flags: sparse,rptree,wildcard |
| Upstream state: None         |
| Upstream neighbor: 192.0.2.4, port: ge-1/3/5.20 |
| Downstream port: ge-1/3/3.20 |
| Downstream neighbors:       |
| 192.0.2.3 State: Join Flags: SRW Timeout: 175 |

user@host> **clear pim snooping join**

Clearing the Join/Prune state for 203.0.113.0/24
Clearing the Join/Prune state for 203.0.113.0/24

user@host> **show pim snooping join extensive**

Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20
clear pim snooping statistics

Syntax

clear pim snooping statistics
<instance instance-name>
@interface interface-name>
<logical-system logical-system-name>
<vlan-id vlan-id>

Release Information
Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

Description
Clear Protocol Independent Multicast (PIM) snooping statistics.

Options

none—Clear PIM snooping statistics for all family addresses, instances, and interfaces.
instance instance-name—(Optional) Clear statistics for a specific PIM-snooping-enabled routing instance.
interface interface-name—(Optional) Clear PIM snooping statistics for a specific interface.
logical-system logical-system-name—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.
vlan-id vlan-identifier—(Optional) Clear PIM snooping statistics information for the specified VLAN.

Required Privilege
Level clear

Related Documentation
• PIM Snooping for VPLS

List of Sample Output

Sample Output
clear pim snooping statistics

The following sample output displays PIM snooping statistics before and after the clear pim snooping statistics command is entered:

user@host> show pim snooping statistics
Instance: vpls1
Learning-Domain: vlan-id 10

See show pim snooping statistics for an explanation of the output fields.
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx J/P messages</td>
<td>0</td>
</tr>
<tr>
<td>RX J/P messages</td>
<td>660</td>
</tr>
<tr>
<td>Rx J/P messages -- seen</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P messages -- received</td>
<td>660</td>
</tr>
<tr>
<td>Rx Hello messages</td>
<td>1396</td>
</tr>
<tr>
<td>Rx Version Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Neighbor Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Upstream Neighbor Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P Busy Drop</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P Group Aggregate</td>
<td>0</td>
</tr>
<tr>
<td>Rx Malformed Packet</td>
<td>0</td>
</tr>
</tbody>
</table>

**Learning-Domain:** vlan-id 20

```
user@host> clear pim snooping statistics
user@host> show pim snooping statistics

Instance: vpls1
Learning-Domain: vlan-id 10

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx J/P messages</td>
<td>0</td>
</tr>
<tr>
<td>RX J/P messages</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P messages -- seen</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P messages -- received</td>
<td>0</td>
</tr>
<tr>
<td>Rx Hello messages</td>
<td>0</td>
</tr>
<tr>
<td>Rx Version Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Neighbor Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Upstream Neighbor Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P Busy Drop</td>
<td>0</td>
</tr>
<tr>
<td>Rx J/P Group Aggregate</td>
<td>0</td>
</tr>
<tr>
<td>Rx Malformed Packet</td>
<td>0</td>
</tr>
</tbody>
</table>

Learning-Domain: vlan-id 20```
clear pim statistics

**List of Syntax**

Syntax on page 1826  
Syntax (EX Series Switch and the QFX Series) on page 1826

**Syntax**

clear pim statistics  
<inet | inet6>  
<instance instance-name>  
<interface interface-name>  
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switch and the QFX Series)**

clear pim statistics  
<inet | inet6>  
<instance instance-name>  
<interface interface-name>

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
*inet6* and *instance* options introduced in Junos OS Release 10.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Clear Protocol Independent Multicast (PIM) statistics.

**Options**

*none*—Clear PIM statistics for all family addresses, instances, and interfaces.  
*inet | inet6*—(Optional) Clear PIM statistics for IPv4 or IPv6 family addresses, respectively.  
*instance instance-name*—(Optional) Clear statistics for a specific PIM-enabled routing instance.  
*interface interface-name*—(Optional) Clear PIM statistics for a specific interface.  
*logical-system (all | logical-system-name)*—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**

The *clear pim statistics* command cannot be used to clear the PIM statistics on a backup Routing Engine when nonstop active routing is enabled.

**Required Privilege Level**

clear

**Related Documentation**

- show pim statistics on page 2018

**List of Sample Output**

clear pim statistics on page 1827
Output Fields  See show pim statistics for an explanation of output fields.

Sample Output

clear pim statistics

The following sample output displays PIM statistics before and after the clear pim statistics command is entered:

user@host> show pim statistics

PIM statistics on all interfaces:  Hello                          0 0 0  
                                      Register                      0 0 0  
                                      Register Stop                 0 0 0  
                                      Join Prune                    0 0 0  
                                      Bootstrap                     0 0 0  
                                      Assert                        0 0 0  
                                      Graft                         0 0 0  
                                      Graft Ack                     0 0 0  
                                      Candidate RP                  0 0 0  
                                      V1 Query                     2111 4222 0  
                                      V1 Register                   0 0 0  
                                      V1 Register Stop              0 0 0  
                                      V1 Join Prune                 14200 13115 0  
                                      V1 RP Reachability            0 0 0  
                                      V1 Assert                     0 0 0  
                                      V1 Graft                      0 0 0  
                                      V1 Graft Ack                  0 0 0  
                                      PIM statistics summary for all interfaces:  Unknown type                            0  
                                      V1 Unknown type                         0  
                                      Unknown Version                         0  
                                      Neighbor unknown                        0  
                                      Bad Length                                0  
                                      Bad Checksum                              0  
                                      Bad Receive If                           0  
                                      Rx Intf disabled                     2007  
                                      Rx V1 Require V2                      0  
                                      Rx V1 Register not RP                   0  
                                      RP Filtered Source                     0  
                                      Unknown Reg Stop                       0  
                                      Rx Join/Prune no state                 1040  
                                      Rx Graft/Graft Ack no state             0  
                                      ...

user@host> clear pim statistics
user@host> show pim statistics

PIM statistics on all interfaces:  Hello                          0 0 0  
                                      Register                      0 0 0  
                                      Register Stop                 0 0 0  
                                      Join Prune                    0 0 0  
                                      Bootstrap                     0 0 0  
                                      Assert                        0 0 0  
                                      Graft                         0 0 0  
                                      Graft Ack                     0 0 0  
                                      Graft Ack                     0 0 0  
                                      Candidate RP                  0 0 0  
                                      V1 Query                     2111 4222 0  
                                      V1 Register                   0 0 0  
                                      V1 Register Stop              0 0 0  
                                      V1 Join Prune                 14200 13115 0  
                                      V1 RP Reachability            0 0 0  
                                      V1 Assert                     0 0 0  
                                      V1 Graft                      0 0 0  
                                      V1 Graft Ack                  0 0 0  
                                      PIM statistics summary for all interfaces:  Unknown type                            0  
                                      V1 Unknown type                         0  
                                      Unknown Version                         0  
                                      Neighbor unknown                        0  
                                      Bad Length                                0  
                                      Bad Checksum                              0  
                                      Bad Receive If                           0  
                                      Rx Intf disabled                     2007  
                                      Rx V1 Require V2                      0  
                                      Rx V1 Register not RP                   0  
                                      RP Filtered Source                     0  
                                      Unknown Reg Stop                       0  
                                      Rx Join/Prune no state                 1040  
                                      Rx Graft/Graft Ack no state             0  
                                      ...

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graft Ack</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Candidate RP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1 Query</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
request pim multicast-tunnel rebalance

### List of Syntax
Syntax on page 1829
Syntax (EX Series Switches) on page 1829

```plaintext
Syntax
request pim multicast-tunnel rebalance
    <instance instance-name>
    <logical-system (all | logical-system-name>)

Syntax (EX Series Switches)
request pim multicast-tunnel rebalance
    <instance instance-name>
```

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

### Description
Rebalance the assignment of multicast tunnel encapsulation interfaces across available tunnel-capable PICs or across a configured list of tunnel-capable PICs. You can determine whether a rebalance is necessary by running the `show pim interfaces instance instance-name` command.

### Options
- **none**—Re-create and rebalance all tunnel interfaces for all routing instances.
- **instance instance-name**—Re-create and rebalance all tunnel interfaces for a specific instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

### Required Privilege Level
maintenance

### Related Documentation
- show pim interfaces on page 1958
- *Load Balancing Multicast Tunnel Interfaces Among Available PICs*

### Output Fields
This command produces no output. To verify the operation of the command, run the `show pim interface instance instance-name` before and after running the `request pim multicast-tunnel rebalance` command.
show amt statistics

Syntax

show amt statistics
<instance instance-name>
<logical-system (all | logical-system-name)>

Release Information

Command introduced in JUNOS Release 10.2.

Description

Display information about the Automatic Multicast Tunneling (AMT) protocol tunnel statistics.

Options

none—Display summary information about all AMT Protocol tunnels.
instance instance-name—(Optional) Display information for the specified instance only.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

Related Documentation

• clear amt statistics on page 1792
• show amt summary on page 1833
• show amt tunnel on page 1835

List of Sample Output

show amt statistics on page 1831

Output Fields

Table 72 on page 1830 describes the output fields for the show amt statistics command. Output fields are listed in the approximate order in which they appear.

Table 72: show amt statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT receive message count</td>
<td>Summary of AMT statistics for messages received on all interfaces.</td>
</tr>
<tr>
<td></td>
<td>• AMT relay discovery—Number of AMT relay discovery messages received.</td>
</tr>
<tr>
<td></td>
<td>• AMT membership request—Number of AMT membership request messages received.</td>
</tr>
<tr>
<td></td>
<td>• AMT membership update—Number of AMT membership update messages received.</td>
</tr>
<tr>
<td>AMT send message count</td>
<td>Summary of AMT statistics for messages sent on all interfaces.</td>
</tr>
<tr>
<td></td>
<td>• AMT relay advertisement—Number of AMT relay advertisement messages sent.</td>
</tr>
<tr>
<td></td>
<td>• AMT membership query—Number of AMT membership query messages sent.</td>
</tr>
</tbody>
</table>
Table 72: show amt statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT error message count</td>
<td>Summary of AMT statistics for error messages received on all interfaces.</td>
</tr>
<tr>
<td>• AMT incomplete packet</td>
<td>Number of messages received with length errors so severe that further classification could not occur.</td>
</tr>
<tr>
<td>• AMT invalid mac</td>
<td>Number of messages received with an invalid message authentication code (MAC).</td>
</tr>
<tr>
<td>• AMT unexpected type</td>
<td>Number of messages received with an unknown message type specified.</td>
</tr>
<tr>
<td>• AMT invalid relay discovery address</td>
<td>Number of AMT relay discovery messages received with an address other than the configured anycast address.</td>
</tr>
<tr>
<td>• AMT invalid membership request address</td>
<td>Number of AMT membership request messages received with an address other than the configured AMT local address.</td>
</tr>
<tr>
<td>• AMT invalid membership update address</td>
<td>Number of AMT membership update messages received with an address other than the configured AMT local address.</td>
</tr>
<tr>
<td>• AMT incomplete relay discovery messages</td>
<td>Number of AMT relay discovery messages received that are not fully formed.</td>
</tr>
<tr>
<td>• AMT incomplete membership request messages</td>
<td>Number of AMT membership request messages received that are not fully formed.</td>
</tr>
<tr>
<td>• AMT incomplete membership update messages</td>
<td>Number of AMT membership update messages received that are not fully formed.</td>
</tr>
<tr>
<td>• AMT no active gateway</td>
<td>Number of AMT membership update messages received for a tunnel that does not exist for the gateway that sent the message.</td>
</tr>
<tr>
<td>• AMT invalid inner header checksum</td>
<td>Number of AMT membership update messages received with an invalid IP checksum.</td>
</tr>
<tr>
<td>• AMT gateways timed out</td>
<td>Number of gateways that timed out because of inactivity.</td>
</tr>
</tbody>
</table>

Sample Output

show amt statistics

```
user@host> show amt statistics

AMT receive message count
AMT relay advertisement : 2
AMT membership request   : 5
AMT membership update    : 5

AMT send message count
AMT relay advertisement : 2
AMT membership query     : 5

AMT error message count
AMT incomplete packet    : 0
AMT invalid mac          : 0
AMT unexpected type      : 0
AMT invalid relay discovery address : 0
AMT invalid membership request address : 0
AMT invalid membership update address : 0
AMT incomplete relay discovery messages : 0
AMT incomplete membership request messages : 0
AMT incomplete membership update messages : 0
AMT no active gateway    : 0
```
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT invalid inner header checksum</td>
<td>0</td>
</tr>
<tr>
<td>AMT gateways timed out</td>
<td>0</td>
</tr>
</tbody>
</table>
show amt summary

Syntax

show amt summary
<instance instance-name>
<logical-system (all | logical-system-name)>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display summary information about the Automatic Multicast Tunneling (AMT) protocol.

Options

none—Display summary information about all AMT protocol instances.

instance instance-name—(Optional) Display information for the specified instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

Related Documentation

- clear amt tunnel on page 1793
- show amt statistics on page 1830
- show amt tunnel on page 1835

List of Sample Output

show amt summary on page 1834

Output Fields

Table 73 on page 1833 describes the output fields for the show amt summary command. Output fields are listed in the approximate order in which they appear.

Table 73: show amt summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT anycast prefix</td>
<td>Prefix advertised by unicast routing protocols to route AMT discovery messages to the router from nearby AMT gateways.</td>
<td>All levels</td>
</tr>
<tr>
<td>AMT anycast address</td>
<td>Anycast address configured from which the anycast prefix is derived.</td>
<td>All levels</td>
</tr>
<tr>
<td>AMT local address</td>
<td>Local unique AMT relay IP address configured. Used to send AMT relay advertisement messages, it is the IP source address of AMT control messages and the source address of the data tunnel encapsulation.</td>
<td>All levels</td>
</tr>
<tr>
<td>AMT tunnel limit</td>
<td>Maximum number of AMT tunnels that can be created.</td>
<td>All levels</td>
</tr>
<tr>
<td>active tunnels</td>
<td>Number of active AMT tunnel interfaces.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Sample Output

show amt summary

```
user@host> show amt summary

  AMT anycast prefix : 20.0.0.4/32
  AMT anycast address : 20.0.0.4
  AMT local address : 20.0.0.4
  AMT tunnel limit : 1000, active tunnels : 2
```
show amt tunnel

Syntax

show amt tunnel
<brief | detail>
<gateway-address gateway-ip-address> <port port-number>
<instance instance-name>
<logical-system (all | logical-system-name)>
<tunnel-interface interface-name>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display information about the Automatic Multicast Tunneling (AMT) dynamic tunnels.

Options

none—Display summary information about all AMT protocol instances.

brief | detail—(Optional) Display the specified level of detail.

gateway-address gateway-ip-address port port-number—(Optional) Display information for the specified AMT gateway only. If no port is specified, display information for all AMT gateways with the given IP address.

instance instance-name—(Optional) Display information for the specified instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

tunnel-interface interface-name—(Optional) Display information for the specified AMT tunnel interface only.

Required Privilege

view

Related Documentation

- clear amt tunnel on page 1793
- show amt statistics on page 1830
- show amt summary on page 1833

List of Sample Output

show amt tunnel on page 1836
show amt tunnel detail on page 1837
show amt tunnel tunnel-interface on page 1837
show amt tunnel gateway-address on page 1837
show amt tunnel gateway-address detail on page 1837

Output Fields

Table 74 on page 1836 describes the output fields for the show amt tunnel command. Output fields are listed in the approximate order in which they appear.
Table 74: show amt tunnel Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMT gateway address</td>
<td>Address of the AMT gateway that is being connected by the AMT tunnel.</td>
<td>All levels</td>
</tr>
<tr>
<td>port</td>
<td>Client port used by the AMT tunnel.</td>
<td>All levels</td>
</tr>
<tr>
<td>AMT tunnel interface</td>
<td>Dynamically created AMT logical interfaces used by the AMT tunnel in the format ud-FPC/PIC/Port.unit.</td>
<td>All levels</td>
</tr>
<tr>
<td>AMT tunnel state</td>
<td>State of the AMT tunnel. The state is normally Active.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Active—The tunnel is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pending—The tunnel creation is pending. This is a transient state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—The tunnel is in the down state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Graceful restart pending—Graceful restart is in progress.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reviving—The routing protocol daemon or Routing Engine was restarted (not gracefully). The tunnel remains in the reviving state until the AMT gateway sends a control message. When the message is received the tunnel is moved to the Active state. If no message is received before the AMT tunnel inactivity timer expires the tunnel is deleted.</td>
<td></td>
</tr>
<tr>
<td>AMT tunnel inactivity timeout</td>
<td>Number of seconds since the most recent control message was received from an AMT gateway. If no message is received before the AMT tunnel inactivity timer expires, the tunnel is deleted.</td>
<td>All levels</td>
</tr>
<tr>
<td>Number of groups</td>
<td>Number of multicast groups using the tunnel.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Multicast group address or addresses using the tunnel.</td>
<td>detail</td>
</tr>
<tr>
<td>Include Source</td>
<td>Multicast source address for each IGMPv3 group using the tunnel.</td>
<td>detail</td>
</tr>
<tr>
<td>AMT message count</td>
<td>Statistics for AMT messages:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• AMT Request—Number of AMT relay tunnel request messages received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AMT membership update—Number of AMT membership update messages received.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show amt tunnel

```
user@host> show amt tunnel
AMT gateway address : 11.11.11.2, port : 2268
AMT tunnel interface : ud-5/1/10.1120256
AMT tunnel state : Active
AMT tunnel inactivity timeout : 15
Number of groups : 1

AMT message count:
AMT Request      AMT membership update
2                2
```
show amt tunnel detail

user@host> show amt tunnel detail
AMT gateway address : 11.11.11.2, port : 2268
AMT tunnel interface : ud-5/3/10.1120512
AMT tunnel state : Active
AMT tunnel inactivity timeout : 62
Number of groups : 1
  Group: 226.2.3.2

AMT message count:
  AMT Request    AMT membership update
  2              2

AMT gateway address : 11.11.11.3, port : 2268
AMT tunnel interface : ud-5/2/10.1120513
AMT tunnel state : Active
AMT tunnel inactivity timeout : 214
Number of groups : 1
  Group: 226.2.3.3

AMT message count:
  AMT Request    AMT membership update
  2              2

show amt tunnel tunnel-interface

user@host> show amt tunnel tunnel-interface ud-5/3/10.1120512
AMT gateway address : 11.11.11.2, port : 2268
AMT tunnel interface : ud-5/3/10.1120512
AMT tunnel state : Active
AMT tunnel inactivity timeout : 145
Number of groups : 1

AMT message count:
  AMT Request    AMT membership update
  2              2

show amt tunnel gateway-address

user@host> show amt tunnel gateway-address 11.11.11.3 port 2268
AMT gateway address : 11.11.11.3, port : 2268
AMT tunnel interface : ud-5/2/10.1120513
AMT tunnel state : Active
AMT tunnel inactivity timeout : 214
Number of groups : 1
  Group: 226.2.3.3

AMT message count:
  AMT Request    AMT membership update
  2              2

show amt tunnel gateway-address detail

user@host> show amt tunnel gateway-address 11.11.11.2 detail

Copyright © 2019, Juniper Networks, Inc.
AMT gateway address: 11.11.11.2, port: 2268
AMT tunnel interface: ud-5/3/10.1120512
AMT tunnel state: Active
AMT tunnel inactivity timeout: 234
Number of groups: 1
  Group: 226.2.3.2

AMT message count:
AMT Request      AMT membership update
   2              2
show dvmrp interfaces

Syntax

show dvmrp interfaces
<logical-system (all | logical-system-name)>

Release Information

NOTE: Distance Vector Multicast Routing Protocol (DVMRP) was deprecated in Junos OS Release 16.1. Although DVMRP commands continue to be available and configurable in the CLI, they are no longer visible and are scheduled for removal in a subsequent release.

Command introduced before Junos OS Release 7.4.

Description

Display information about Distance Vector Multicast Routing Protocol (DVMRP)–enabled interfaces.

Options

none—(Same as logical-system all) Display information about DVMRP-enabled interfaces.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show dvmrp interfaces on page 1841

Output Fields

Table 75 on page 1839 describes the output fields for the show dvmrp interfaces command. Output fields are listed in the approximate order in which they appear.

Table 75: show dvmrp interfaces 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>
<tr>
<td>State</td>
<td>State of the interface: up or down.</td>
</tr>
<tr>
<td>Leaf</td>
<td>Whether the interface is a leaf (that is, whether it has no neighbors) or whether it has neighbors.</td>
</tr>
<tr>
<td>Metric</td>
<td>Interface metric: a value from 1 through 31.</td>
</tr>
<tr>
<td>Announce</td>
<td>Number of routes the interface is announcing.</td>
</tr>
</tbody>
</table>
Table 75: show dvmrp interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>DVMRP mode:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forwarding</strong>—DVMRP does both the routing and the multicast data forwarding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unicast-routing</strong>—DVMRP does only the routing. Forwarding of the multicast data packets can be done by enabling PIM on the interface.</td>
</tr>
</tbody>
</table>
Sample Output

show dvmrp interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Leaf</th>
<th>Metric</th>
<th>Announce</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>fxp0.0</td>
<td>Up</td>
<td>N</td>
<td>1</td>
<td>4</td>
<td>Forwarding</td>
</tr>
<tr>
<td>fxp1.0</td>
<td>Up</td>
<td>N</td>
<td>1</td>
<td>4</td>
<td>Forwarding</td>
</tr>
<tr>
<td>fxp2.0</td>
<td>Up</td>
<td>N</td>
<td>1</td>
<td>3</td>
<td>Forwarding</td>
</tr>
<tr>
<td>lo0.0</td>
<td>Up</td>
<td>Y</td>
<td>1</td>
<td>0</td>
<td>Unicast-routing</td>
</tr>
</tbody>
</table>
show dvmrp neighbors

Syntax

```
show dvmrp neighbors
<logical-system (all | logical-system-name)>
```

Release Information

NOTE: Distance Vector Multicast Routing Protocol (DVMRP) was deprecated in Junos OS Release 16.1. Although DVMRP commands continue to be available and configurable in the CLI, they are no longer visible and are scheduled for removal in a subsequent release.

Command introduced before Junos OS Release 7.4.

Description

Display information about Distance Vector Multicast Routing Protocol (DVMRP) neighbors.

Options

```
none—(Same as logical-system all) Display information about DVMRP neighbors.
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 dvmrp neighbors on page 1843

Output Fields

Table 76 on page 1842 describes the output fields for the show dvmrp neighbors command. Output fields are listed in the approximate order in which they appear.

Table 76: show dvmrp neighbors Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Address of the neighboring DVMRP router.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of DVMRP that the neighbor is running, in the format <code>major.minor</code>.</td>
</tr>
</tbody>
</table>
Table 76: `show dvmrp neighbors` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Information about the neighbor:</td>
</tr>
<tr>
<td></td>
<td>• 1 — One way. The local router has seen the neighbor, but the neighbor has not seen the local router.</td>
</tr>
<tr>
<td></td>
<td>• G — Neighbor supports generation ID.</td>
</tr>
<tr>
<td></td>
<td>• L — Neighbor is a leaf router.</td>
</tr>
<tr>
<td></td>
<td>• M — Neighbor supports mtrace.</td>
</tr>
<tr>
<td></td>
<td>• N — Neighbor supports netmask in prune messages and graft messages.</td>
</tr>
<tr>
<td></td>
<td>• P — Neighbor supports pruning.</td>
</tr>
<tr>
<td></td>
<td>• S — Neighbor supports SNMP.</td>
</tr>
<tr>
<td>Routes</td>
<td>Number of routes learned from the neighbor.</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the DVMRP neighbor information times out, in seconds.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Number of generation ID changes that have occurred since the local router learned about the neighbor.</td>
</tr>
</tbody>
</table>

Sample Output

`show dvmrp neighbors`

```
user@host> show dvmrp neighbors

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Interface</th>
<th>Version</th>
<th>Flags</th>
<th>Routes</th>
<th>Timeout</th>
<th>Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>ipip.0</td>
<td>3.255</td>
<td>PGM</td>
<td>3</td>
<td>28</td>
<td>1</td>
</tr>
</tbody>
</table>
```
**show dvmrp prefix**

**Syntax**

```
show dvmrp prefix
  <brief | detail>
  <logical-system (all | logical-system-name)>
  <prefix>
```

**Release Information**

NOTE: Distance Vector Multicast Routing Protocol (DVMRP) was deprecated in Junos OS Release 16.1. Although DVMRP commands continue to be available and configurable in the CLI, they are no longer visible and are scheduled for removal in a subsequent release.

Command introduced before Junos OS Release 7.4.

**Description**

Display information about Distance Vector Multicast Routing Protocol (DVMRP) prefixes.

**Options**

**none**—Display standard information about all DVMRP prefixes.

**brief | detail**—(Optional) Display the specified level of output.

**logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**prefix**—(Optional) Display information about specific prefixes.

**Required Privilege**

view

**List of Sample Output**

- show dvmrp prefix on page 1846
- show dvmrp prefix brief on page 1846
- show dvmrp prefix detail on page 1846

**Output Fields**

Table 77 on page 1844 describes the output fields for the show dvmrp prefix 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>Prefix</td>
<td>DVMRP route.</td>
<td>All levels</td>
</tr>
<tr>
<td>Next hop</td>
<td>Next hop from which the route was learned.</td>
<td>All levels</td>
</tr>
<tr>
<td>Age</td>
<td>Last time that the route was refreshed.</td>
<td>All levels</td>
</tr>
<tr>
<td>multicast-group</td>
<td>Multicast group address.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 77: show dvmrp prefix Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prunes sent</td>
<td>Number of prune messages sent to the multicast group.</td>
<td>detail</td>
</tr>
<tr>
<td>Grafts sent</td>
<td>Number of grafts sent to the multicast group.</td>
<td>detail</td>
</tr>
<tr>
<td>Cache lifetime</td>
<td>Lifetime of the group in the multicast cache, in seconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Prune lifetime</td>
<td>Lifetime remaining and total lifetime of prune messages, in seconds.</td>
<td>detail</td>
</tr>
</tbody>
</table>
### Sample Output

**show dvmrp prefix**

```bash
user@host> show dvmrp prefix
```

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next hop</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.38.0.0/30</td>
<td>10.38.0.1</td>
<td>00:06:17</td>
</tr>
<tr>
<td>10.38.0.4/30</td>
<td>10.38.0.5</td>
<td>00:06:13</td>
</tr>
<tr>
<td>10.38.0.8/30</td>
<td>10.38.0.2</td>
<td>00:00:04</td>
</tr>
<tr>
<td>10.38.0.12/30</td>
<td>10.38.0.6</td>
<td>00:00:04</td>
</tr>
<tr>
<td>10.255.14.142/32</td>
<td>10.38.0.2</td>
<td>00:00:04</td>
</tr>
<tr>
<td>10.255.14.144/32</td>
<td>10.38.0.2</td>
<td>00:00:04</td>
</tr>
<tr>
<td>10.255.70.15/32</td>
<td>10.38.0.6</td>
<td>00:00:04</td>
</tr>
<tr>
<td>192.168.195.40/30</td>
<td>192.168.195.41</td>
<td>00:06:17</td>
</tr>
<tr>
<td>192.168.195.92/30</td>
<td>10.38.0.2</td>
<td>00:00:04</td>
</tr>
</tbody>
</table>

**show dvmrp prefix brief**

The output for the `show dvmrp prefix brief` command is identical to that for the `show dvmrp prefix` command.

**show dvmrp prefix detail**

```bash
user@host> show dvmrp prefix detail
```

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next hop</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.38.0.0/30</td>
<td>10.38.0.1</td>
<td>00:06:28</td>
</tr>
<tr>
<td>10.38.0.4/30</td>
<td>10.38.0.5</td>
<td>00:06:24</td>
</tr>
<tr>
<td>10.38.0.8/30</td>
<td>10.38.0.2</td>
<td>00:00:15</td>
</tr>
<tr>
<td>10.38.0.12/30</td>
<td>10.38.0.6</td>
<td>00:00:15</td>
</tr>
<tr>
<td>10.255.14.142/32</td>
<td>10.38.0.2</td>
<td>00:00:15</td>
</tr>
<tr>
<td>10.255.14.144/32</td>
<td>10.38.0.2</td>
<td>00:00:15</td>
</tr>
<tr>
<td>10.255.70.15/32</td>
<td>10.38.0.6</td>
<td>00:00:15</td>
</tr>
<tr>
<td>192.168.195.40/30</td>
<td>192.168.195.41</td>
<td>00:06:28</td>
</tr>
<tr>
<td>192.168.195.92/30</td>
<td>10.38.0.2</td>
<td>00:00:15</td>
</tr>
</tbody>
</table>
show dvmrp prunes

**Syntax**

```
show dvmrp prunes
  <all | rx | tx>
  <logical-system (all | logical-system-name)>
```

**Release Information**

NOTE: Distance Vector Multicast Routing Protocol (DVMRP) was deprecated in Junos OS Release 16.1. Although DVMRP commands continue to be available and configurable in the CLI, they are no longer visible and are scheduled for removal in a subsequent release.

Command introduced before Junos OS Release 7.4.

**Description**

Display information about active Distance Vector Multicast Routing Protocol (DVMRP) prune messages.

**Options**

- **none**—Display received and transmitted DVMRP prune information.
- **all**—(Optional) Display information about all received and transmitted prune messages.
- **rx**—(Optional) Display information about received prune messages.
- **tx**—(Optional) Display information about transmitted prune messages.
- **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 dvmrp prunes on page 1848

**Output Fields**

Table 78 on page 1847 describes the output fields for the show dvmrp prunes command. Output fields are listed in the approximate order in which they appear.

**Table 78: show dvmrp prunes Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Group address.</td>
</tr>
<tr>
<td>Source prefix</td>
<td>Prefix for the prune.</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the prune message expires, in seconds.</td>
</tr>
</tbody>
</table>
### Table 78: show dvmrp prunes Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Neighbor to which the prune was sent or from which the prune was received.</td>
</tr>
</tbody>
</table>

#### Sample Output

**show dvmrp prunes**

```
user@host> show dvmrp prunes
```

<table>
<thead>
<tr>
<th>Group</th>
<th>Source prefix</th>
<th>Timeout</th>
<th>Neighbor</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.1.1</td>
<td>128.112.0.0</td>
<td>/12</td>
<td>7077 192.168.1.1</td>
</tr>
<tr>
<td>224.0.1.32</td>
<td>160.0.0.0</td>
<td>/3</td>
<td>7087 192.168.1.1</td>
</tr>
<tr>
<td>224.2.123.4</td>
<td>136.0.0.0</td>
<td>/5</td>
<td>6955 192.168.1.1</td>
</tr>
<tr>
<td>224.2.127.1</td>
<td>129.0.0.0</td>
<td>/8</td>
<td>7046 192.168.1.1</td>
</tr>
<tr>
<td>224.2.135.86</td>
<td>128.102.128.0</td>
<td>/17</td>
<td>7071 192.168.1.1</td>
</tr>
<tr>
<td>224.2.135.86</td>
<td>129.0.0.0</td>
<td>/8</td>
<td>7074 192.168.1.1</td>
</tr>
<tr>
<td>224.2.135.86</td>
<td>130.0.0.0</td>
<td>/7</td>
<td>7071 192.168.1.1</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show igmp group

List of Syntax  Syntax on page 1849
               Syntax (EX Series Switch and the QFX Series) on page 1849

Syntax  show igmp group
           <brief | detail>
           <group-name>
           <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)  show igmp group
                                               <brief | detail>
                                               <group-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 11.3 for the QFX Series.
                        Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Display Internet Group Management Protocol (IGMP) group membership information.

Options  none—Display standard information about membership for all IGMP groups.
          brief | detail—(Optional) Display the specified level of output.
          group-name—(Optional) Display group membership for the specified IP address only.
          logical-system (all | logical-system-name)—(Optional) Perform this operation on all
                                             logical systems or on a particular logical system.

Required Privilege  Level  view

Related Documentation  • clear igmp membership on page 1795

List of Sample Output  show igmp group (Include Mode) on page 1850
                       show igmp group (Exclude Mode) on page 1851
                       show igmp group brief on page 1851
                       show igmp group detail on page 1851

Output Fields  Table 79 on page 1850 describes the output fields for the show igmp group command.
               Output fields are listed in the approximate order in which they appear.
### Table 79: show igmp group 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 the interface that received the IGMP membership report. A name of local indicates that the local routing device joined the group itself.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group Mode</td>
<td>Mode the SSM group is operating in: Include or Exclude.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Source address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source timeout</td>
<td>Time remaining until the group traffic is no longer forwarded. The timer is refreshed when a listener in include mode sends a report. A group in exclude mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Last reported by</td>
<td>Address of the host that last reported membership in this group.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time remaining until the group membership is removed.</td>
<td>brief none</td>
</tr>
<tr>
<td>Group timeout</td>
<td>Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>Type of group membership:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Dynamic—Host reported the membership.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Static—Membership is configured.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

**show igmp group (Include Mode)**

```
user@host> show igmp group

Interface: t1-0/1/0.0
Group: 198.51.100.1  
  Group mode: Include  
  Source: 203.0.113.2  
  Last reported by: 203.0.113.52  
  Timeout: 24 Type: Dynamic
Group: 198.51.100.1  
  Group mode: Include  
  Source: 203.0.113.3  
  Last reported by: 203.0.113.52  
  Timeout: 24 Type: Dynamic
Group: 198.51.100.1  
  Group mode: Include  
  Source: 203.0.113.4  
  Last reported by: 203.0.113.52  
  Timeout: 24 Type: Dynamic
Group: 198.51.100.1  
  Group mode: Include  
  Source: 203.0.113.4
```
show igmp group

user@host> show igmp group

Interface: t1-0/1/0.0
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 198.51.100.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout: 0 Type: Dynamic
  Group: 198.51.100.22
    Source: 0.0.0.0
    Last reported by: Local
    Timeout: 0 Type: Dynamic

show igmp group brief

The output for the show igmp group brief command is identical to that for the show igmp group command.

show igmp group detail

user@host> show igmp group detail

Interface: t1-0/1/0.0
  Group: 198.51.100.1
    Group mode: Include
    Source: 203.0.113.2
    Source timeout: 12
    Last reported by: 203.0.113.52
    Group timeout: 0 Type: Dynamic
  Group: 198.51.100.1
    Group mode: Include
    Source: 203.0.113.3
    Source timeout: 12
    Last reported by: 203.0.113.52
    Group timeout: 0 Type: Dynamic
  Group: 198.51.100.1
    Group mode: Include
    Source: 203.0.113.4
<table>
<thead>
<tr>
<th>Source timeout</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reported by</td>
<td>203.0.113.52</td>
</tr>
<tr>
<td>Group timeout</td>
<td>0</td>
</tr>
<tr>
<td><strong>Group: 198.51.100.2</strong></td>
<td></td>
</tr>
<tr>
<td>Group mode:</td>
<td>Include</td>
</tr>
<tr>
<td>Source:</td>
<td>203.0.113.4</td>
</tr>
<tr>
<td>Source timeout:</td>
<td>12</td>
</tr>
<tr>
<td>Last reported by:</td>
<td>203.0.113.52</td>
</tr>
<tr>
<td>Group timeout:</td>
<td>0</td>
</tr>
<tr>
<td><strong>Interface: t1-0/1/1.0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Interface: ge-0/2/2.0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Interface: ge-0/2/0.0</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Interface: local</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Group: 198.51.100.12</strong></td>
<td></td>
</tr>
<tr>
<td>Group mode:</td>
<td>Exclude</td>
</tr>
<tr>
<td>Source:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Source timeout:</td>
<td>0</td>
</tr>
<tr>
<td>Last reported by:</td>
<td>Local</td>
</tr>
<tr>
<td>Group timeout:</td>
<td>0</td>
</tr>
<tr>
<td><strong>Group: 198.51.100.22</strong></td>
<td></td>
</tr>
<tr>
<td>Group mode:</td>
<td>Exclude</td>
</tr>
<tr>
<td>Source:</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Source timeout:</td>
<td>0</td>
</tr>
<tr>
<td>Last reported by:</td>
<td>Local</td>
</tr>
<tr>
<td>Group timeout:</td>
<td>0</td>
</tr>
</tbody>
</table>
**show igmp interface**

**List of Syntax**  
Syntax on page 1853  
Syntax (EX Series Switches and the QFX Series) on page 1853

**Syntax**

```
show igmp interface
  <brief | detail>
  <interface-name>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and the QFX Series)**

```
show igmp interface
  <brief | detail>
  <interface-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 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**  
Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.

**Options**

- `none`—Display standard information about all IGMP-enabled interfaces.
- `brief | detail`—(Optional) Display the specified level of output.
- `interface-name`—(Optional) Display information about the specified IGMP-enabled interface only.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**  
view

**Related Documentation**

- clear igmp membership on page 1795

**List of Sample Output**

- show igmp interface on page 1855
- show igmp interface brief on page 1856
- show igmp interface detail on page 1856
- show igmp interface <interface-name> on page 1856

**Output Fields**  
Table 80 on page 1854 describes the output fields for the `show igmp interface` command. Output fields are listed in the approximate order in which they appear.
Table 80: show igmp 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>Name of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Querier</td>
<td>Address of the routing device that has been elected to send membership queries.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: <strong>Up</strong> or <strong>Down</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>SSM Map Policy</td>
<td>Name of the source-specific multicast (SSM) map policy that has been applied to the IGMP interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the IGMP querier is declared to be unreachable, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Version</td>
<td>IGMP version being used on the interface: 1, 2, or 3.</td>
<td>All levels</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group limit</td>
<td>Maximum number of groups allowed on the interface. Any joins requested after the limit is reached are rejected.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group threshold</td>
<td>Configured threshold at which a warning message is generated.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group log-interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
<td>All levels</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>State of the immediate leave option:</td>
<td>All levels</td>
</tr>
<tr>
<td>Promiscuous Mode</td>
<td>State of the promiscuous mode option:</td>
<td>All levels</td>
</tr>
<tr>
<td>Distributed</td>
<td>State of IGMP, which, by default, takes place on the Routing Engine for MX Series routers but can be distributed to the Packet Forwarding Engine to provide faster processing of join and leave events.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

- **On**—indicates that the router removes a host from the multicast group as soon as the router receives a leave group message from a host associated with the interface.
- **Off**—indicates that after receiving a leave group message, instead of removing a host from the multicast group immediately, the router sends a group query to determine if another receiver responds.

- **On**—indicates that the router can accept IGMP reports from subnetworks that are not associated with its interfaces.
- **Off**—indicates that the router can accept IGMP reports only from subnetworks that are associated with its interfaces.
Table 80: show igmp 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>Passive</td>
<td>State of the passive mode option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router can run IGMP on the interface but not send or receive control traffic such as IGMP reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that the router can run IGMP on the interface and send or receive control traffic such as IGMP reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td>OIF map</td>
<td>Name of the OIF map (if configured) associated with the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>SSM map</td>
<td>Name of the source-specific multicast (SSM) map (if configured) used on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Configured Parameters</td>
<td>Information configured by the user:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• IGMP Query Interval—Interval (in seconds) at which this router sends membership queries when it is the querier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IGMP Query Response Interval—Time (in seconds) that the router waits for a report in response to a general query.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IGMP Last Member Query Interval—Time (in seconds) that the router waits for a report in response to a group-specific query.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IGMP Robustness Count—Number of times the router retries a query.</td>
<td></td>
</tr>
<tr>
<td>Derived Parameters</td>
<td>Derived information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• IGMP Membership Timeout—Timeout period (in seconds) for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IGMP Other Querier Present Timeout—Time (in seconds) that the router waits for the IGMP querier to send a query.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

```
show igmp interface
```

```
user@host> show igmp interface
Interface: at-0/3/1.0
    Querier: 203.0.3.113.31
    State: Up Timeout: None Version: 2 Groups: 4
    SSM Map Policy: ssm-policy-A
Interface: so-1/0/0.0
    Querier: 203.0.113.11
    State: Up Timeout: None Version: 2 Groups: 2
    SSM Map Policy: ssm-policy-B
```
Interface: so-1/0/1.0
   Querier: 203.0.113.21
   State: Up Timeout: None Version: 2 Groups: 4
   SSM Map Policy: ssm-policy-C
   Immediate Leave: On
   Promiscuous Mode: Off
   Passive: Off
   Distributed: On

Configured Parameters:
   IGMP Query Interval: 125.0
   IGMP Query Response Interval: 10.0
   IGMP Last Member Query Interval: 1.0
   IGMP Robustness Count: 2

Derived Parameters:
   IGMP Membership Timeout: 260.0
   IGMP Other Querier Present Timeout: 255.0

show igmp interface brief

The output for the show igmp interface brief command is identical to that for the show igmp interface command. For sample output, see show igmp interface on page 1855.

show igmp interface detail

The output for the show igmp interface detail command is identical to that for the show igmp interface command. For sample output, see show igmp interface on page 1855.

show igmp interface <interface-name>

user@host# show igmp interface ge-3/2/0.0

Interface: ge-3/2/0.0
   Querier: 203.0.113.111
   State: Up Timeout: None
   Version: 3
   Groups: 1
   Group limit: 8
   Group threshold: 60
   Group log-interval: 10
   Immediate leave: Off
   Promiscuous mode: Off
   Distributed: On
show igmp snooping interface

Syntax

show igmp snooping interface interface-name
<brief | detail>
<bridge-domain bridge-domain-name>
<logical-system logical-system-name>
<virtual-switch virtual-switch-name>
<vlan-id vlan-identifier>

Release Information

Command introduced in Junos OS Release 8.5.

Description

Display IGMP snooping interface information.

Options

none — Display detailed information.

brief | detail—(Optional) When applicable, this option lets you choose the how much detail to display.

bridge-domain bridge-domain-name—(Optional) Display information about a particular bridge domain.

logical-system logical-system-name—(Optional) Display information about a particular logical system, or type ‘all’.

virtual-switch virtual-switch-name—(Optional) Display information about a particular virtual switch.

vlan-id vlan-identifier—(Optional) Display information about a particular VLAN.

Required Privilege

view

Related Documentation

• show igmp snooping membership on page 1863
• show igmp snooping statistics on page 1869

List of Sample Output

show igmp snooping interface on page 1859
show igmp snooping interface (logical systems) on page 1859
show igmp snooping interface (Group Limit Configured) on page 1861
show igmp snooping interface (ELS EX Series switches with MVR configured) on page 1862

Output Fields

Table 81 on page 1858 lists the output fields for the show igmp snooping interface 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>Routing-instance or instance</td>
<td>Routing instance for IGMP snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Bridge Domain or Vlan</td>
<td>Bridge domain or VLAN for which IGMP snooping is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Learning Domain</td>
<td>Learning domain for snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>interface</td>
<td>Interfaces that are being snooped in this learning domain.</td>
<td>All levels</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: <strong>Up</strong> or <strong>Down</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Up Groups</td>
<td>Number of active multicast groups attached to the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>immediate-leave</td>
<td>State of immediate leave: <strong>On</strong> or <strong>Off</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>router-interface</td>
<td>Router interfaces that are part of this learning domain.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group limit</td>
<td>Maximum number of (source, group) pairs allowed per interface. When a group limit is not configured, this field is not shown.</td>
<td>All levels</td>
</tr>
<tr>
<td>Data-forwarding receiver: yes</td>
<td>VLAN associated with the interface is configured as a data-forwarding multicast receiver VLAN using multicast VLAN registration (MVR) on EX Series switches with Enhanced Layer 2 Software (ELS).</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Query interval</td>
<td>Frequency (in seconds) with which this router sends membership queries when it is the querier.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Query Response Interval</td>
<td>Time (in seconds) that the router waits for a response to a general query.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Last Member Query Interval</td>
<td>Time (in seconds) that the router waits for a report in response to a group-specific query.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Robustness Count</td>
<td>Number of times the router retries a query.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Membership Timeout</td>
<td>Timeout for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Other Querier Present Timeout</td>
<td>Time that the router waits for the IGMP querier to send a query.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Sample Output

show igmp snooping interface

user@host> show igmp snooping interface ge-0/1/4

Instance: default-switch
Bridge-Domain: sample
Learning-Domain: default
Interface: ge-0/1/4.0
State: Up Groups: 0
Immediate leave: Off
Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Derived Parameters:
IGMP Membership Timeout: 260.0
IGMP Other Querier Present Timeout: 255.0

show igmp snooping interface (logical systems)

user@host> show igmp snooping interface logical-system all

logical-system: default
Instance: VPLS-6
Learning-Domain: default
Interface: ge-0/2/2.601
  State: Up Groups: 10
  Immediate leave: Off
  Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Instance: VS-4
Bridge-Domain: VS-4-BD-1
Learning-Domain: vlan-id 1041
Interface: ae2.3
  State: Up Groups: 0
  Immediate leave: Off
  Router interface: no

Interface: ge-0/2/2.1041
  State: Up Groups: 20
  Immediate leave: Off
  Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
<table>
<thead>
<tr>
<th>Instance</th>
<th>Bridge-Domain</th>
<th>Learning-Domain</th>
<th>Interface</th>
<th>State</th>
<th>Groups</th>
<th>Immediate Leave</th>
<th>Router Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-switch</td>
<td>bd-200</td>
<td>default</td>
<td>ge-0/2/2.100</td>
<td>Up</td>
<td>20</td>
<td>Off</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configured Parameters:</td>
<td></td>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bd0</td>
<td></td>
<td>default</td>
<td>ae0.0</td>
<td>Up</td>
<td>0</td>
<td>Off</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ae1.0</td>
<td>Up</td>
<td>0</td>
<td>Off</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/2/2.0</td>
<td>Up</td>
<td>32</td>
<td>Off</td>
<td>no</td>
</tr>
<tr>
<td>Configured Parameters:</td>
<td></td>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPLS-1</td>
<td></td>
<td>default</td>
<td>ge-0/2/2.502</td>
<td>Up</td>
<td>11</td>
<td>Off</td>
<td>no</td>
</tr>
<tr>
<td>Configured Parameters:</td>
<td></td>
<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>
<td></td>
<td></td>
</tr>
<tr>
<td>VS-1</td>
<td></td>
<td>default</td>
<td>ge-0/2/2.1010</td>
<td>Up</td>
<td>20</td>
<td>Off</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Bridge-Domain: VS-BD-2
Learning-Domain: default
Interface: ae2.0
  State: Up Groups: 0
  Immediate leave: Off
  Router interface: no

Interface: ge-0/2/2.1011
  State: Up Groups: 20
  Immediate leave: Off
  Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Instance: VPLS-p2mp
Learning-Domain: default
Interface: ge-0/2/2.3001
  State: Up Groups: 0
  Immediate leave: Off
  Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

show igmp snooping interface (Group Limit Configured)

user@host> show igmp snooping interface instance vpls1

Instance: vpls1

Learning-Domain: default
Interface: ge-1/3/9.0
  State: Up Groups: 0
  Immediate leave: Off
  Router interface: yes

Interface: ge-1/3/8.0
  State: Up Groups: 0
  Immediate leave: Off
  Router interface: yes
  Group limit: 1000

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
show igmp snooping interface (ELS EX Series switches with MVR configured)

<table>
<thead>
<tr>
<th>Instance: inst1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan: v2</td>
</tr>
<tr>
<td>Learning-Domain: default</td>
</tr>
<tr>
<td>Interface: ge-0/0/0.0</td>
</tr>
<tr>
<td>State: Up Groups: 0</td>
</tr>
<tr>
<td>Immediate leave: Off</td>
</tr>
<tr>
<td>Router interface: no</td>
</tr>
<tr>
<td>Group limit: 3</td>
</tr>
<tr>
<td>Data-forwarding receiver: yes</td>
</tr>
</tbody>
</table>
show igmp snooping membership

Syntax

```plaintext
show igmp snooping membership
  <brief | detail>
  <instance routing-instance-name>
  <interface interface-name>
  <vlan (vlan-id | vlan-name)>
  <bridge-domain bridge-domain-name>
  <group group-name>
  <logical-system logical-system-name>
  <virtual-switch virtual-switch-name>
  <vlan-id vlan-identifier>
```

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 18.1R1 for the SRX1500 devices.

Description

Display the multicast group membership information maintained by IGMP snooping.

Options

- **none**—Display the multicast group membership information about all VLANs on which IGMP snooping is enabled.
- **brief | detail**—(Optional) Display the specified level of output. The default is **brief**.

```
NOTE: On QFX Series switches, the output is the same for either brief or detail levels.
```

- **instance routing-instance-name**—(Optional) Display the multicast group membership information about the specified routing instance.
- **interface interface-name**—(Optional) Display the multicast group membership information about the specified interface.
- **vlan (vlan-id | vlan-name)**—(Optional) Display the multicast group membership for the specified VLAN.
- **bridge-domain bridge-domain-name**—(Optional) Display information about a particular bridge domain.
- **group group-name**—(Optional) Display information about this group address.
- **logical-system logical-system-name**—(Optional) Display information about a particular logical system, or type ‘all’.
- **virtual-switch virtual-switch-name**—(Optional) Display information about a particular virtual switch.
- **vlan-id vlan-identifier**—(Optional) Display information about a particular VLAN.
Required Privilege
Level

view

Related Documentation
• show igmp snooping interface on page 1857
• show igmp snooping statistics on page 1869
• clear igmp snooping membership on page 1798

List of Sample Output
show igmp snooping membership on page 1865
show igmp snooping membership (SRX1500) on page 1866
show igmp snooping membership detail (SRX1500) on page 1866
show igmp snooping membership (Exclude Mode) on page 1866
show igmp snooping membership interface ge-0/1/2.200 on page 1867
show igmp snooping membership vlan-id 1 on page 1867
show igmp snooping membership (ELS EX Series switches with MVR) on page 1867
show igmp snooping membership <detail> (QFX5100 switches—same output with or without detail option) on page 1868

Output Fields
Table 82 on page 1864 lists the output fields for the show igmp snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 82: show igmp snooping membership Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
<td>All</td>
</tr>
<tr>
<td>Instance</td>
<td>Routing instance for IGMP snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Learning Domain</td>
<td>Learning domain for snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which this router is a proxy.</td>
<td>detail</td>
</tr>
<tr>
<td>Data-forwarding receiver: yes</td>
<td>(EX Series switches with Enhanced Layer 2 Software (ELS) only) VLAN associated with the interface is configured as a data-forwarding multicast receiver VLAN using multicast VLAN registration (MVR).</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Interfaces configured on MVR receiver VLANs are listed under the associated MVR source VLAN (MVLAN) for which the interface forwards multicast streams.</td>
<td></td>
</tr>
<tr>
<td>Up Groups or Groups</td>
<td>Number of active multicast groups attached to the logical interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 82: `show igmp snooping membership` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>(Not displayed on QFX Series switches) IP multicast address of the multicast group.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>The following information is provided for the multicast group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Last reporter—Last host to report membership for the multicast group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Receiver count—Number of hosts on the interface that are members of the multicast group (field appears only if <code>immediate-leave</code> is configured on the VLAN), or number of interfaces that have membership in a multicast group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Uptime—Length of time (in hours, minutes, and seconds) a multicast group has been active on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• timeout—Time (in seconds) left until the entry for the multicast group is removed from the multicast group if no membership reports are received on the interface. This counter is reset to its maximum value when a membership report is received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flags—The lowest IGMP version in use by a host that is a member of the group on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Include source—Source addresses from which multicast streams are allowed based on IGMPv3 reports.</td>
<td></td>
</tr>
<tr>
<td>Group Mode</td>
<td>Mode the SSM group is operating in: Include or Exclude.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Source address used on queries.</td>
<td>All levels</td>
</tr>
<tr>
<td>Last reported by</td>
<td>Address of source last replying to the query.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group Timeout</td>
<td>Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>Length of time (in seconds) left until the entry is purged.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>Way that the group membership information was learned:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Dynamic—Group membership was learned by the IGMP protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Static—Group membership was learned by configuration.</td>
<td></td>
</tr>
<tr>
<td>Include receiver</td>
<td>Source address of receiver included in membership with timeout (in seconds).</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

`show igmp snooping membership`

```
user@host> show igmp snooping membership
Instance: vpls2
Learning-Domain: vlan-id 2
Interface: ge-3/0/0.2
Up Groups: 0
Interface: ge-3/1/0.2
```
show igmp snooping membership (SRX1500)

```
user@host> show igmp snooping membership

Instance: default-switch

Vlan: v1

Learning-Domain: default
Interface: ge-0/0/3.0, Groups: 1
Group: 233.252.0.100
Group mode: Exclude
Source: 0.0.0.0
Last reported by: Local
Group timeout: 0 Type: Static
```

show igmp snooping membership detail (SRX1500)

```
user@host> show igmp snooping membership detail

VLAN: vlan2 Tag: 2 (Index: 3)
Router interfaces:
  ge-1/0/0.0 dynamic Uptime: 00:14:24 timeout: 253
Group: 233.252.0.99
  ge-1/0/17.0 259 Last reporter: 10.0.0.90 Receiver count: 1
  Uptime: 00:00:19 timeout: 259 Flags: <V3-hosts>
    Include source: 10.2.11.5, 10.2.11.12
```

show igmp snooping membership (Exclude Mode)

```
user@host> show igmp snooping membership

Instance: vpls1

Learning-Domain: vlan-id 1
Interface: ge-3/0/0.1
Up Groups: 0
Interface: ge-3/1/0.1
Up Groups: 0
Interface: ge-3/1/5.1
Up Groups: 1
  Group: 233.252.0.99
    Group mode: Exclude
    Source: 0.0.0.0
    Last reported by: 233.252.0.87
    Group timeout: 173 Type: Dynamic
```
show igmp snooping membership interface ge-0/1/2.200

user@host> show igmp snooping membership interface ge-0/1/2.200

Instance: bridge-domain bar

Learning-Domain: default
Interface: ge-0/1/2.200
  Group: 233.252.0.1
    Source: 0.0.0.0
    Timeout: 391 Type: Static
  Group: 232.1.1.1
    Source: 192.128.1.1
    Timeout: 0 Type: Static

show igmp snooping membership vlan-id 1

user@host> show igmp snooping membership vlan-id 1

Instance: vpls2

Instance: vpls1

Learning-Domain: vlan-id 1
Interface: ge-3/0/0.1
Up Groups: 0
Interface: ge-3/1/0.1
Up Groups: 0
Interface: ge-3/1/5.1
Up Groups: 1
  Group: 233.252.0.1
    Group mode: Exclude
    Source: 0.0.0.0
    Last reported by: 233.252.0.82
    Group timeout: 173 Type: Dynamic

show igmp snooping membership (ELS EX Series switches with MVR)

user@host> show igmp snooping membership
Instance: default-switch
Vlan: v2

Learning-Domain: default
Interface: ge-0/0/0.0, Groups: 0
Data-forwarding receiver: yes

Learning-Domain: default
Interface: ge-0/0/12.0, Groups: 1
Group: 233.252.0.1
  Group mode: Exclude
  Source: 0.0.0.0
  Last reported by: Local
  Group timeout: 0 Type: Static

show igmp snooping membership <detail> (QFX5100 switches—same output with or without detail option)

user@host> show igmp snooping membership detail

Instance: default-switch
Vlan: v100

Learning-Domain: default
Interface: xe-0/0/51:0.0, Groups: 1
Group: 233.252.0.1
  Group mode: Exclude
  Source: 0.0.0.0
  Last reported by: 233.252.0.82
  Group timeout: 251 Type: Dynamic
**show igmp snooping statistics**

**Syntax**

```
show igmp snooping statistics
<brief | detail>
<bridge-domain bridge-domain-name>
<logical-system logical-system-name>
<virtual-switch virtual-switch-name>
<vlan-id vlan-identifier>
```

**Release Information**

Command introduced in Junos OS Release 8.5.  
Command introduced in Junos OS Release 18.1R1 for the SR1500 devices.

**Description**

Display IGMP snooping statistics.

**Options**

- `none` — (Optional) Display detailed information.
- `brief | detail` — (Optional) Display the specified level of output.
- `bridge-domain bridge-domain-name` — (Optional) Display information about a particular bridge domain.
- `logical-system logical-system-name` — (Optional) Display information about a particular logical system, or type 'all'.
- `virtual-switch virtual-switch-name` — (Optional) Display information about a particular virtual switch.
- `vlan-id vlan-identifier` — (Optional) Display information about a particular VLAN.

**Required Privilege**

- `view` Level

**Related Documentation**

- `show igmp snooping interface` on page 1857
- `show igmp snooping membership` on page 1863
- `clear igmp snooping statistics` on page 1800

**List of Sample Output**

- `show igmp snooping statistics` on page 1871
- `show igmp snooping statistics (SRX1500)` on page 1871
- `show igmp snooping statistics logical-systems all` on page 1872
- `show igmp snooping statistics interface (Bridge Domains Configured)` on page 1873

**Output Fields**

Table 83 on page 1870 lists the output fields for the `show igmp snooping statistics` command.  
Output fields are listed in the approximate order in which they appear.
Table 83: `show igmp snooping statistics` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing-instance</td>
<td>Routing instance for IGMP snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP packet</td>
<td>Heading for IGMP snooping statistics for all interfaces or for the specified interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>learning-domain</td>
<td>Appears at end of “IGMP packets statistics” line.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Message type</td>
<td>Summary of IGMP statistics:</td>
<td>All levels</td>
</tr>
<tr>
<td>Received</td>
<td>Number of messages received.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of messages sent.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx errors</td>
<td>Number of received packets that contained errors.</td>
<td>All levels</td>
</tr>
<tr>
<td>IGMP Global</td>
<td>Summary of IGMP snooping statistics for all interfaces.</td>
<td>All levels</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Membership Query—Number of membership queries sent and received.
- V1 Membership Report—Number of version 1 membership reports sent and received.
- DVMRP—Number of DVMRP messages sent or received.
- PIM V1—Number of PIM version 1 messages sent or received.
- Cisco Trace—Number of Cisco trace messages sent or received.
- V2 Membership Report—Number of version 2 membership reports sent or received.
- Group Leave—Number of group leave messages sent or received.
- Domain Wide Report—Number of domain-wide reports sent or received.
- V3 Membership Report—Number of version 3 membership reports sent or received.
- Other Unknown types—Number of unknown message types received.
- IGMP v3 unsupported type—Number of messages received with unknown and unsupported IGMP version 3 message types.
- IGMP v3 source required for SSM—Number of IGMP version 3 messages received that contained no source.
- IGMP v3 mode not applicable for SSM—Number of IGMP version 3 messages received that did not contain a mode applicable for source-specific multicast (SSM).
Sample Output

`show igmp snooping statistics`  

```
user@host> show igmp snooping statistics

Routing-instance foo

IGMP packet statistics for all interfaces in learning-domain vlan-100

<table>
<thead>
<tr>
<th>IGMP Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Query</td>
<td>89</td>
<td>51</td>
<td>0</td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVMPR</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM V1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td>139</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td>136</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 unsupported type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 source required for SSM</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 mode not applicable for SSM</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IGMP Global Statistics

Bad Length: 0
Bad Checksum: 0
Rx non-local: 0

Routing-instance bar

IGMP packet statistics for all interfaces in learning-domain vlan-100

<table>
<thead>
<tr>
<th>IGMP Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Query</td>
<td>89</td>
<td>51</td>
<td>0</td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DVMPR</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM V1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td>139</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td>136</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 unsupported type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 source required for SSM</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 mode not applicable for SSM</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IGMP Global Statistics

Bad Length: 0
Bad Checksum: 0
Rx non-local: 0
```

```
show igmp snooping statistics (SRX1500)

user@host> show igmp snooping statistics

Vlan: v1

<table>
<thead>
<tr>
<th>IGMP Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Query</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVMPR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIM V1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Trace</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Leave</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Unknown types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 unsupported type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 source required for SSM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP v3 mode not applicable for SSM</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

```
Chapter 19: IP Multicast Operational Commands

Copyright © 2019, Juniper Networks, Inc.

```
show igmp snooping statistics logical-systems all

<table>
<thead>
<tr>
<th>Logical System</th>
<th>IGMP Message Type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Membership Query</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>DVMRP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>PIM V1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V2 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Request</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Domain Wide Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V3 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Other Unknown types</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Learning-Domain: vlan-id 1041 bridge-domain VS-4-BD-1

<table>
<thead>
<tr>
<th>Logical System</th>
<th>IGMP Message Type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Membership Query</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>DVMRP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>PIM V1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V2 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Request</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Domain Wide Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V3 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Other Unknown types</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Bridge: VPLS-p2mp

<table>
<thead>
<tr>
<th>Logical System</th>
<th>IGMP Message Type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Membership Query</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V1 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>DVMRP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>PIM V1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Cisco Trace</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>V2 Membership Report</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Group Leave</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Response</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Mtrace Request</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Other Unknown types</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show igmp snooping statistics interface (Bridge Domains Configured)

user@host> show igmp snooping statistics interface

<table>
<thead>
<tr>
<th>Bridge: bridge-domain1</th>
<th>IGMP interface packet statistics for ge-2/0/8.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Message type</td>
<td>Received</td>
</tr>
<tr>
<td>Membership Query</td>
<td>0</td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP</td>
<td>0</td>
</tr>
<tr>
<td>PIM V1</td>
<td>0</td>
</tr>
<tr>
<td>Cisco Trace</td>
<td>0</td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>Group Leave</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Response</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Request</td>
<td>0</td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td>0</td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge: bridge-domain2</th>
<th>IGMP interface packet statistics for ge-2/0/8.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Message type</td>
<td>Received</td>
</tr>
<tr>
<td>Membership Query</td>
<td>0</td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP</td>
<td>0</td>
</tr>
<tr>
<td>PIM V1</td>
<td>0</td>
</tr>
<tr>
<td>Cisco Trace</td>
<td>0</td>
</tr>
<tr>
<td>V2 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>Group Leave</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Response</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace Request</td>
<td>0</td>
</tr>
<tr>
<td>Domain Wide Report</td>
<td>0</td>
</tr>
<tr>
<td>V3 Membership Report</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td>0</td>
</tr>
</tbody>
</table>
**show igmp statistics**

**List of Syntax**

Syntax on page 1874
Syntax (EX Series Switch and the QFX Series) on page 1874

**Syntax**

```
show igmp statistics
  <brief | detail>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show igmp statistics
  <brief | detail>
  <interface interface-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display Internet Group Management Protocol (IGMP) statistics.

**Options**

`none`—Display IGMP statistics for all interfaces.

`brief | detail`—(Optional) Display the specified level of output.

`interface interface-name`—(Optional) Display IGMP statistics about the specified interface only.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

`view`

**Related Documentation**

- clear igmp statistics on page 1801

**List of Sample Output**

show igmp statistics on page 1876
show igmp statistics interface on page 1876

**Output Fields**

Table 84 on page 1875 describes the output fields for the `show igmp statistics` command. Output fields are listed in the approximate order in which they appear.
Table 84: show igmp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP packet statistics</td>
<td>Heading for IGMP packet statistics for all interfaces or for the specified interface name.</td>
</tr>
<tr>
<td>IGMP Message type</td>
<td>Summary of IGMP statistics:</td>
</tr>
<tr>
<td></td>
<td>• Membership Query—Number of membership queries sent and received.</td>
</tr>
<tr>
<td></td>
<td>• V1 Membership Report—Number of version 1 membership reports sent and received.</td>
</tr>
<tr>
<td></td>
<td>• DVMRP—Number of DVMRP messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• PIM V1—Number of PIM version 1 messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Trace—Number of Cisco trace messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• V2 Membership Report—Number of version 2 membership reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Group Leave—Number of group leave messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Mtrace Response—Number of Mtrace response messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Mtrace Request—Number of Mtrace request messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Domain Wide Report—Number of domain-wide reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• V3 Membership Report—Number of version 3 membership reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Other Unknown types—Number of unknown message types received.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 unsupported type—Number of messages received with unknown and unsupported IGMP version 3 message types.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 source required for SSM—Number of IGMP version 3 messages received that contained no source.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 mode not applicable for SSM—Number of IGMP version 3 messages received that did not contain a mode applicable for source-specific multicast (SSM). Beginning with certain releases, this type includes records received for groups in the SSM range of addresses and in which the mode is MODE_IS_EXCLUDE or CHANGE_TO_EXCLUDE_MODE. This includes records with a non-empty source list.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of messages received.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of messages sent.</td>
</tr>
<tr>
<td>Rx errors</td>
<td>Number of received packets that contained errors.</td>
</tr>
<tr>
<td>Max Rx rate (pps)</td>
<td>Maximum number of IGMP packets received during 1 second interval.</td>
</tr>
<tr>
<td>IGMP Global Statistics</td>
<td>Summary of IGMP statistics for all interfaces.</td>
</tr>
<tr>
<td></td>
<td>• Bad Length—Number of messages received with length errors so severe that further classification could not occur.</td>
</tr>
<tr>
<td></td>
<td>• Bad Checksum—Number of messages received with a bad IP checksum. No further classification was performed.</td>
</tr>
<tr>
<td></td>
<td>• Bad Receive If—Number of messages received on an interface not enabled for IGMP.</td>
</tr>
<tr>
<td></td>
<td>• Rx non-local—Number of messages received from senders that are not local.</td>
</tr>
<tr>
<td></td>
<td>• Timed out—Number of groups that timed out as a result of not receiving an explicit leave message.</td>
</tr>
<tr>
<td></td>
<td>• Rejected Report—Number of reports dropped because of the IGMP group policy.</td>
</tr>
<tr>
<td></td>
<td>• Total Interfaces—Number of interfaces configured to support IGMP.</td>
</tr>
</tbody>
</table>
Sample Output

**show igmp statistics**

```plaintext
user@host> show igmp statistics

IGMP packet statistics for all interfaces
IGMP Message type       Received  Sent  Rx errors
Membership Query         8883      459    0
V1 Membership Report     0         0      0
DVMRP                    0         0      0
PIM V1                   0         0      0
Cisco Trace              0         0      0
V2 Membership Report     0         0      0
Group Leave              0         0      0
Mtrace Response          0         0      0
Mtrace Request           0         0      0
Domain Wide Report       0         0      0
V3 Membership Report     0         0      0
Other Unknown types      0
IGMP v3 unsupported type 0
IGMP v3 source required for SSM 0
IGMP v3 mode not applicable for SSM 0

IGMP Global Statistics
Bad Length                0
Bad Checksum              0
Bad Receive If            0
Rx non-local              1227
Timed out                 0
Rejected Report           0
Total Interfaces          2
Max Rx rate (pps)         1536
```

**show igmp statistics interface**

```plaintext
user@host> show igmp statistics interface fe-1/0/1.0

IGMP interface packet statistics for fe-1/0/1.0
IGMP Message type       Received  Sent  Rx errors
Membership Query         0         230    0
V1 Membership Report     0         0      0
```

```
show mld group

Syntax
show mld group
  <brief | detail>
  <group-name>
  <logical-system (all | logical-system-name)>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Display information about Multicast Listener Discovery (MLD) group membership.

Options
none—Display standard information about all MLD groups.

brief | detail—(Optional) Display the specified level of output.

group-name—(Optional) Display MLD information about the specified group.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

Related Documentation
• clear mld membership on page 1803

List of Sample Output
show mld group (Include Mode) on page 1878
show mld group (Exclude Mode) on page 1879
show mld group brief on page 1879
show mld group detail (Include Mode) on page 1879
show mld group detail (Exclude Mode) on page 1880

Output Fields
Table 85 on page 1877 describes the output fields for the show mld group command. Output fields are listed in the approximate order in which they appear.

Table 85: show mld group 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 the interface that received the MLD membership report; local means that the local router joined the group itself.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Source address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group Mode</td>
<td>Mode the SSM group is operating in: Include or Exclude.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 85: show mld group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reported by</td>
<td>Address of the host that last reported membership in this group.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source timeout</td>
<td>Time remaining until the group traffic is no longer forwarded. The timer is refreshed when a listener in include mode sends a report. A group in exclude mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time remaining until the group membership is removed.</td>
<td>brief none</td>
</tr>
<tr>
<td>Group timeout</td>
<td>Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>Type of group membership:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Dynamic—Host reported the membership.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Static—Membership is configured.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show mld group
(Include Mode)

```
user@host> show mld group

Interface: fe-0/1/2.0
  Group: ff02::1:ff05:1a67
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout: 245 Type: Dynamic
  Group: ff02::1:ffa8:c35e
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout: 241 Type: Dynamic
  Group: ff02::2:43e:d7f6
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout: 244 Type: Dynamic
Group: ff05::2
  Group mode: Include
  Source: ::
  Last reported by: fe80::2e0:81ff:fe05:1a67
  Timeout: 244 Type: Dynamic
Interface: local
  Group: ff02::2
    Source: ::
    Last reported by: Local
    Timeout: 0 Type: Dynamic
  Group: ff02::16
    Source: ::
```
show mld group (Exclude Mode)

```shell
user@host> show mld group
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
  Group: ff02::6
    Source: ::
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Timeout:     245 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Timeout:     28 Type: Dynamic
Interface: local
  Group: ff02::2
    Source: ::
    Last reported by: Local
    Timeout:       0 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: Local
    Timeout:       0 Type: Dynamic
```

show mld group brief

The output for the `show mld group brief` command is identical to that for the `show mld group` command. For sample output, see `show mld group (Include Mode)` on page 1878 and `show mld group (Exclude Mode)` on page 1879.

show mld group detail (Include Mode)

```shell
user@host> show mld group detail
Interface: fe-0/1/2.0
  Group: ff02::1:ff05:1a67
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:     224 Type: Dynamic
  Group: ff02::1:ffa8:c35e
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:     220 Type: Dynamic
  Group: ff02::2:43e:d7f6
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:     223 Type: Dynamic
  Group: ff05::2
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:     223 Type: Dynamic
```
Interface: so-1/0/1.0
  Group: ff02::2
    Group mode: Include
    Source: ::
    Last reported by: fe80::280:42ff:fe15:f445
    Timeout:  258 Type: Dynamic

Interface: local
  Group: ff02::2
    Group mode: Include
    Source: ::
    Last reported by: Local
    Timeout:  0 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: Local
    Timeout:  0 Type: Dynamic

show mld group detail (Exclude Mode)

user@host> show mld group detail

Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
  Group: ff02::6
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Group timeout:  226 Type: Dynamic
  Group: ff02::16
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Group timeout:  246 Type: Dynamic

Interface: local
  Group: ff02::2
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: Local
    Group timeout:  0 Type: Dynamic
  Group: ff02::16
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: Local
    Group timeout:  0 Type: Dynamic
**show mld interface**

**Syntax**

```
show mld interface
  <brief | detail>
  <interface-name>
  <logical-system (all | logical-system-name)>
```

**Release Information**
Command introduced before Junos OS Release 7.4.

**Description**
Display information about multipoint Listener Discovery (MLD)-enabled interfaces.

**Options**

- **none**—Display standard information about all MLD-enabled interfaces.
- **brief | detail**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display information about the specified interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- **Level**
  - view

**Related Documentation**
- clear mld membership on page 1803

**List of Sample Output**

- show mld interface on page 1883
- show mld interface brief on page 1884
- show mld interface detail on page 1884
- show mld interface <interface-name> on page 1884

**Output Fields**

Table 86 on page 1881 describes the output fields for the `show mld interface` 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>Interface</td>
<td>Name of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Querier</td>
<td>Address of the router that has been elected to send membership queries.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: <strong>Up</strong> or <strong>Down</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>SSM Map Policy</td>
<td>Name of the source-specific multicast (SSM) map policy that has been applied to the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>SSM Map Policy</td>
<td>Name of the source-specific multicast (SSM) map policy at the MLD interface.</td>
<td>All levels</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>Timeout</td>
<td>How long until the MLD querier is declared to be unreachable, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Version</td>
<td>MLD version being used on the interface: 1 or 2.</td>
<td>All levels</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Passive</td>
<td>State of the passive mode option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router can run IGMP or MLD on the interface but not send or receive control traffic such as IGMP or MLD reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that the router can run IGMP or MLD on the interface and send or receive control traffic such as IGMP or MLD reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The passive statement enables you to selectively activate up to two out of a possible three available query or control traffic options. When enabled, the following options appear after the on state declaration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• send-general-query—The interface sends general queries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• send-group-query—The interface sends group-specific and group-source-specific queries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• allow-receive—The interface receives control traffic</td>
<td></td>
</tr>
<tr>
<td>OIF map</td>
<td>Name of the OIF map associated to the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>SSM map</td>
<td>Name of the source-specific multicast (SSM) map used on the interface, if configured.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group limit</td>
<td>Maximum number of groups allowed on the interface. Any memberships requested after the limit is reached are rejected.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group threshold</td>
<td>Configured threshold at which a warning message is generated.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group log-interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
<td>All levels</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>State of the immediate leave option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router removes a host from the multicast group as soon as the router receives a multicast listener done message from a host associated with the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that after receiving a multicast listener done message, instead of removing a host from the multicast group immediately, the router sends a group query to determine if another receiver responds.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 86: show mld 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>Distributed</td>
<td>State of MLD, which, by default, takes place on the Routing Engine for MX Series routers but can be distributed to the Packet Forwarding Engine to provide faster processing of join and leave events.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—distributed MLD is enabled.</td>
<td></td>
</tr>
<tr>
<td>Configured Parameters</td>
<td>Information configured by the user.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• MLD Query Interval (.1 secs)—Interval at which this router sends membership queries when it is the querier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MLD Query Response Interval (.1 secs)—Time that the router waits for a report in response to a general query.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MLD Last Member Query Interval (.1 secs)—Time that the router waits for a report in response to a group-specific query.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MLD Robustness Count—Number of times the router retries a query.</td>
<td></td>
</tr>
<tr>
<td>Derived Parameters</td>
<td>Derived information.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• MLD Membership Timeout (.1 secs)—Timeout period for group membership. If no report is received for these groups before the timeout expires, the group membership will be removed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MLD Other Querier Present Timeout (.1 secs)—Time that the router waits for the IGMP querier to send a query.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

```
show mld interface

  user@host> show mld interface

  Interface: fe-0/0/0
     Querier: None
     State: Up      Timeout: 0    Version: 1    Groups: 0
     SSM Map Policy: ssm-policy-A
  Interface: at-0/3/1.0
     Querier: 8038::c0a8:c345
     State: Up      Timeout: None   Version: 1    Groups: 0
     SSM Map Policy: ssm-policy-B
  Interface: fe-1/0/1.0
     Querier: ::192.168.195.73
     State: Up      Timeout: None   Version: 1    Groups: 3
     SSM Map Policy: ssm-policy-C
     SSM map: ipv6map1
  Immediate Leave: On
  Promiscuous Mode: Off
  Passive: Off
  Distributed: On

  Configured Parameters:
  MLD Query Interval (.1 secs): 1250
  MLD Query Response Interval (.1 secs): 100
  MLD Last Member Query Interval (.1 secs): 10
  MLD Robustness Count: 2
```
show mld interface brief

The output for the `show mld interface brief` command is identical to that for the `show mld interface` command. For sample output, see `show mld interface` on page 1883.

show mld interface detail

The output for the `show mld interface detail` command is identical to that for the `show mld interface` command. For sample output, see `show mld interface` on page 1883.

show mld interface <interface-name>

```
user@host# show mld interface ge-3/2/0.0
Interface: ge-3/2/0.0
     Querier: 203.0.113.111
     State: Up   Timeout: None  Version: 3  Groups: 1
     Group limit: 8
     Group threshold: 60
     Group log-interval: 10
     Immediate leave: Off
     Promiscuous mode: Off  Distributed: On
```
show mld statistics

Syntax

show mld statistics
<interface interface-name>
<logical-system (all | logical-system-name)>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Display information about Multicast Listener Discovery (MLD) statistics.

Options

none—Display MLD statistics for all interfaces.

interface interface-name—(Optional) Display statistics about the specified interface.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

Related Documentation
- clear mld statistics on page 1804

List of Sample Output
- show mld statistics on page 1886
- show mld statistics interface on page 1887

Output Fields
Table 87 on page 1885 describes the output fields for the show mld statistics command. Output fields are listed in the approximate order in which they appear.

Table 87: show mld statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>Number of received packets.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of transmitted packets.</td>
</tr>
<tr>
<td>Rx errors</td>
<td>Number of received packets that contained errors.</td>
</tr>
</tbody>
</table>
Table 87: show mld statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MLD Message type</strong></td>
<td>Summary of MLD statistics.</td>
</tr>
<tr>
<td>• Listener Query (v1/v2)</td>
<td>Number of membership queries sent and received.</td>
</tr>
<tr>
<td>• Listener Report (v1)</td>
<td>Number of version 1 membership reports sent and received.</td>
</tr>
<tr>
<td>• Listener Done (v1/v2)</td>
<td>Number of Listener Done messages sent and received.</td>
</tr>
<tr>
<td>• Listener Report (v2)</td>
<td>Number of version 2 membership reports sent and received.</td>
</tr>
<tr>
<td>• Other Unknown types</td>
<td>Number of unknown message types received.</td>
</tr>
<tr>
<td>• MLD v2 source required for SSM</td>
<td>Number of MLD version 2 messages received that contained no source.</td>
</tr>
<tr>
<td>• MLD v2 mode not applicable for SSM</td>
<td>Number of MLD version 2 messages received that did not contain a mode applicable for source-specific multicast (SSM).</td>
</tr>
<tr>
<td><strong>MLD Global Statistics</strong></td>
<td>Summary of MLD statistics for all interfaces.</td>
</tr>
<tr>
<td>• Bad Length</td>
<td>Number of messages received with length errors so severe that further classification could not occur.</td>
</tr>
<tr>
<td>• Bad Checksum</td>
<td>Number of messages received with an invalid IP checksum. No further classification was performed.</td>
</tr>
<tr>
<td>• Bad Receive If</td>
<td>Number of messages received on an interface not enabled for MLD.</td>
</tr>
<tr>
<td>• Rx non-local</td>
<td>Number of messages received from nonlocal senders.</td>
</tr>
<tr>
<td>• Timed out</td>
<td>Number of groups that timed out as a result of not receiving an explicit leave message.</td>
</tr>
<tr>
<td>• Rejected Report</td>
<td>Number of reports dropped because of the MLD group policy.</td>
</tr>
<tr>
<td>• Total Interfaces</td>
<td>Number of interfaces configured to support IGMP.</td>
</tr>
</tbody>
</table>

Sample Output

show mld statistics

```
user@host> show mld statistics

MLD packet statistics for all interfaces

<table>
<thead>
<tr>
<th>MLD Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener Query (v1/v2)</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Listener Report (v1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Listener Done (v1/v2)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Listener Report (v2)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Unknown types</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLD v2 source required for SSM</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLD v2 mode not applicable for SSM</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MLD Global Statistics

<table>
<thead>
<tr>
<th>MLD Global Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>0</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show mld statistics interface

```
show mld statistics interface fe-1/0/1.0

MLD interface packet statistics for fe-1/0/1.0
MLD Message type    Received  Sent  Rx errors
Listener Query (v1/v2) 0      2      0
Listener Report (v1) 0      0      0
Listener Done (v1/v2) 0      0      0
Listener Report (v2) 0      0      0
Other Unknown types 0
MLD v2 source required for SSM 2
MLD v2 mode not applicable for SSM 0

MLD Global Statistics
Bad Length 0
Bad Checksum 0
Bad Receive If 0
Rx non-local 0
Timed out 0
Rejected Report 0
Total Interfaces 2
```
**show msdp**

**Syntax**

```
show msdp
  <brief | detail>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <peer peer-address>
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 12.1 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display Multicast Source Discovery Protocol (MSDP) information.

**Options**

- **none**—Display standard MSDP information for all routing instances.
- **brief | detail**—(Optional) Display the specified level of output.
- **instance instance-name**—(Optional) Display information for the specified instance only.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **peer peer-address**—(Optional) Display information about the specified peer only.

**Required Privilege Level**

- **view**

**Related Documentation**

- show msdp source on page 1891
- show msdp source-active on page 1893
- show msdp statistics on page 1896

**List of Sample Output**

- show msdp on page 1889
- show msdp brief on page 1889
- show msdp detail on page 1889

**Output Fields**

Table 88 on page 1888 describes the output fields for the `show msdp` command. Output fields are listed in the approximate order in which they appear.

### Table 88: show msdp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer address</td>
<td>IP address of the peer.</td>
<td>All levels</td>
</tr>
<tr>
<td>Local address</td>
<td>Local address of the peer.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 88: show msdp 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>Status of the MSDP connection: Listen, Established, or Inactive.</td>
<td>All levels</td>
</tr>
<tr>
<td>Last up/down</td>
<td>Time at which the most recent peer-state change occurred.</td>
<td>All levels</td>
</tr>
<tr>
<td>Peer-Group</td>
<td>Peer group name.</td>
<td>All levels</td>
</tr>
<tr>
<td>SA Count</td>
<td>Number of source-active cache entries advertised by each peer that were accepted, compared to the number that were received, in the format number-accepted/number-received.</td>
<td>All levels</td>
</tr>
<tr>
<td>Peer Connect Retries</td>
<td>Number of peer connection retries.</td>
<td>detail</td>
</tr>
<tr>
<td>State timer expires</td>
<td>Number of seconds before another message is sent to a peer.</td>
<td>detail</td>
</tr>
<tr>
<td>Peer Times out</td>
<td>Number of seconds to wait for a response from the peer before the peer is declared unavailable.</td>
<td>detail</td>
</tr>
<tr>
<td>SA accepted</td>
<td>Number of entries in the source-active cache accepted from the peer.</td>
<td>detail</td>
</tr>
<tr>
<td>SA received</td>
<td>Number of entries in the source-active cache received by the peer.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show msdp

```
user@host> show msdp
Peer address    Local address   State       Last up/down Peer-Group SA Count
198.32.8.193    198.32.8.195    Established  5d 19:25:44 North23    120/150
198.32.8.194    198.32.8.195    Established  3d 19:27:27 North23    300/345
198.32.8.196    198.32.8.195    Established  5d 19:39:36 North23    10/13
198.32.8.197    198.32.8.195    Established  5d 19:32:27 North23    5/6
198.32.8.198    198.32.8.195    Established  3d 19:33:04 North23    2305/3000
```

show msdp brief

The output for the show msdp brief command is identical to that for the show msdp command. For sample output, see show msdp on page 1889.

show msdp detail

```
user@host> show msdp detail
Peer: 10.255.70.15
Local address: 10.255.70.19
State: Established
Peer Connect Retries: 0
State timer expires: 22
Peer Times out: 49
```
SA accepted: 0
SA received: 0
show msdp source

**Syntax**

`show msdp source
<instance instance-name>
<logical-system (all | logical-system-name)>
<source-address>`

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display multicast sources learned from Multicast Source Discovery Protocol (MSDP).

**Options**

none—Display standard MSDP source information for all routing instances.

_instance instance-name_—(Optional) Display information for the specified instance only.

_logical-system (all | logical-system-name)_—(Optional) Perform this operation on all logical systems or on a particular logical system.

_source-address_—(Optional) IP address and optional prefix length. Display information for the specified source address only.

**Required Privilege Level**

view

**Related Documentation**

- show msdp on page 1888
- show msdp source-active on page 1893
- show msdp statistics on page 1896

**List of Sample Output**

show msdp source on page 1892
Output Fields  Table 89 on page 1892 describes the output fields for the `show msdp source` command. Output fields are listed in the approximate order in which they appear.

Table 89: show msdp source Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>IP address of the source.</td>
</tr>
<tr>
<td>/Len</td>
<td>Length of the prefix for this IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>Discovery method for this multicast source:</td>
</tr>
<tr>
<td></td>
<td>• Configured—Source-active limit explicitly configured for this source.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic—Source-active limit established when this source was discovered.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Source-active limit applied to this source.</td>
</tr>
<tr>
<td>Threshold</td>
<td>Source-active threshold applied to this source.</td>
</tr>
<tr>
<td>Exceeded</td>
<td>Number of source-active messages received from this source exceeding the established maximum.</td>
</tr>
</tbody>
</table>

Sample Output

```
show msdp source
```

```
user@host> show msdp source

<table>
<thead>
<tr>
<th>Source address</th>
<th>/Len</th>
<th>Type</th>
<th>Maximum</th>
<th>Threshold</th>
<th>Exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>/0</td>
<td>Configured</td>
<td>5</td>
<td>none</td>
<td>0</td>
</tr>
<tr>
<td>10.1.0.0</td>
<td>/16</td>
<td>Configured</td>
<td>500</td>
<td>none</td>
<td>0</td>
</tr>
<tr>
<td>10.1.1.1</td>
<td>/32</td>
<td>Configured</td>
<td>10000</td>
<td>none</td>
<td>0</td>
</tr>
<tr>
<td>10.1.1.2</td>
<td>/32</td>
<td>Dynamic</td>
<td>6936</td>
<td>none</td>
<td>0</td>
</tr>
<tr>
<td>10.1.5.5</td>
<td>/32</td>
<td>Dynamic</td>
<td>500</td>
<td>none</td>
<td>123</td>
</tr>
<tr>
<td>10.2.1.1</td>
<td>/32</td>
<td>Dynamic</td>
<td>2</td>
<td>none</td>
<td>0</td>
</tr>
</tbody>
</table>
```
**show msdp source-active**

**Syntax**
```
show msdp source-active
  <brief | detail>
  <group group>
  <instance instance-name>
  <local>
  <logical-system (all | logical-system-name)>
  <originator originator>
  <peer peer-address>
  <source source-address>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display the Multicast Source Discovery Protocol (MSDP) source-active cache.

**Options**
- **none**—Display standard MSDP source-active cache information for all routing instances.
- **brief | detail**—(Optional) Display the specified level of output.
- **group group**—(Optional) Display source-active cache information for the specified group.
- **instance instance-name**—(Optional) Display information for the specified instance.
- **local**—(Optional) Display all source-active caches originated by this router.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **originator originator**—(Optional) Display information about the peer that originated the source-active cache entries.
- **peer peer-address**—(Optional) Display the source-active cache of the specified peer.
- **source source-address**—(Optional) Display the source-active cache of the specified source.

**Required Privilege Level**
view

**Related Documentation**
- show msdp on page 1888
- show msdp source on page 1891
- show msdp statistics on page 1896

**List of Sample Output**
show msdp source-active on page 1894
show msdp source-active brief on page 1895
show msdp source-active detail on page 1895
show msdp source-active source on page 1895

Output Fields

Table 90 on page 1894 describes the output fields for the `show msdp source-active` command. Output fields are listed in the approximate order in which they appear.

**Table 90: show msdp source-active Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global active source limit exceeded</td>
<td>Number of times all peers have exceeded configured active source limits.</td>
</tr>
<tr>
<td>Configured number of active source messages accepted by the device.</td>
<td>Configured number of active source messages accepted by the device.</td>
</tr>
<tr>
<td>Configured threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.</td>
<td>Configured threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.</td>
</tr>
<tr>
<td>Threshold at which a warning message is logged (percentage of the number of active source messages accepted by the device).</td>
<td>Threshold at which a warning message is logged (percentage of the number of active source messages accepted by the device).</td>
</tr>
<tr>
<td>Time (in seconds) between consecutive log messages.</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>Multicast address of the group.</td>
<td>Group address</td>
</tr>
<tr>
<td>IP address of the source.</td>
<td>Source address</td>
</tr>
<tr>
<td>IP address of the peer.</td>
<td>Peer address</td>
</tr>
<tr>
<td>Router ID configured on the source of the rendezvous point (RP) that originated the message, or the loopback address when the router ID is not configured.</td>
<td>Originator</td>
</tr>
<tr>
<td>Flags: Accept, Reject, or Filtered.</td>
<td>Flags</td>
</tr>
</tbody>
</table>

Sample Output

```
show msdp source-active

user@host> show msdp source-active

  Group address   Source address  Peer address    Originator      Flags
  230.0.0.0       192.168.195.46  local           10.255.14.30    Accept
  230.0.0.1       192.168.195.46  local           10.255.14.30    Accept
  230.0.0.2       192.168.195.46  local           10.255.14.30    Accept
  230.0.0.3       192.168.195.46  local           10.255.14.30    Accept
  230.0.0.4       192.168.195.46  local           10.255.14.30    Accept
```
show msdp source-active brief

The output for the `show msdp source-active brief` command is identical to that for the `show msdp source-active` command. For sample output, see `show msdp source-active` on page 1894.

show msdp source-active detail

The output for the `show msdp source-active detail` command is identical to that for the `show msdp source-active` command. For sample output, see `show msdp source-active` on page 1894.

show msdp source-active source

```
user@host>  show msdp source-active source 192.168.215.246

Global active source limit exceeded: 0
Global active source limit maximum: 25000
Global active source limit threshold: 24000
Global active source limit log-warning: 100
Global active source limit log interval: 0

<table>
<thead>
<tr>
<th>Group address</th>
<th>Source address</th>
<th>Peer address</th>
<th>Originator</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>226.2.2.1</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.3</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.4</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.5</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.7</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.10</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.11</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.13</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.14</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
<tr>
<td>226.2.2.15</td>
<td>192.168.215.246</td>
<td>10.255.182.140</td>
<td>10.255.182.140</td>
<td>Accept</td>
</tr>
</tbody>
</table>
```
### show msdp statistics

**Syntax**

```
show msdp statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
<peer peer-address>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 12.1 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display statistics about Multicast Source Discovery Protocol (MSDP) peers.

**Options**

- `none`—Display statistics about all MSDP peers for all routing instances.
- `instance instance-name`—(Optional) Display statistics about a specific MSDP instance.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `peer peer-address`—(Optional) Display statistics about a particular MSDP peer.

**Required Privilege**

- **Level**: `view`

**Related Documentation**

- clear msdp statistics on page 1806
- show msdp statistics on page 1898
- show msdp statistics peer on page 1898

**List of Sample Output**

- show msdp statistics on page 1898
- show msdp statistics peer on page 1898

**Output Fields**

Table 91 on page 1896 describes the output fields for the `show msdp statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 91: show msdp statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global active source limit exceeded</td>
<td>Number of times all peers have exceeded configured active source limits.</td>
</tr>
<tr>
<td>Global active source limit maximum</td>
<td>Configured number of active source messages accepted by the device.</td>
</tr>
<tr>
<td>Global active source limit threshold</td>
<td>Configured threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.</td>
</tr>
<tr>
<td>Global active source limit log-warning</td>
<td>Threshold at which a warning message is logged (percentage of the number of active source messages accepted by the device).</td>
</tr>
</tbody>
</table>
Table 9: show msdp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global active source limit log interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>Peer</td>
<td>Address of peer.</td>
</tr>
<tr>
<td>Last State Change</td>
<td>How long ago the peer state changed.</td>
</tr>
<tr>
<td>Last message received from the peer</td>
<td>How long ago the last message was received from the peer.</td>
</tr>
<tr>
<td>RPF Failures</td>
<td>Number of reverse path forwarding (RPF) failures.</td>
</tr>
<tr>
<td>Remote Closes</td>
<td>Number of times the remote peer closed.</td>
</tr>
<tr>
<td>Peer Timeouts</td>
<td>Number of peer timeouts.</td>
</tr>
<tr>
<td>SA messages sent</td>
<td>Number of source-active messages sent.</td>
</tr>
<tr>
<td>SA messages received</td>
<td>Number of source-active messages received.</td>
</tr>
<tr>
<td>SA request messages sent</td>
<td>Number of source-active request messages sent.</td>
</tr>
<tr>
<td>SA request messages received</td>
<td>Number of source-active request messages received.</td>
</tr>
<tr>
<td>SA response messages sent</td>
<td>Number of source-active response messages sent.</td>
</tr>
<tr>
<td>SA response messages received</td>
<td>Number of source-active response messages received.</td>
</tr>
<tr>
<td>SA messages with zero Entry Count received</td>
<td>Entry Count is a field within SA message that defines how many source/group tuples are present in the SA message. The counter is incremented each time an SA with an Entry Count of zero is received.</td>
</tr>
<tr>
<td>Active source exceeded</td>
<td>Number of times this peer has exceeded configured source-active limits.</td>
</tr>
<tr>
<td>Active source Maximum</td>
<td>Configured number of active source messages accepted by this peer.</td>
</tr>
<tr>
<td>Active source threshold</td>
<td>Configured threshold on this peer for applying random early discard (RED) to drop some but not all MSDP active source messages.</td>
</tr>
<tr>
<td>Active source log-warning</td>
<td>Configured threshold on this peer at which a warning message is logged (percentage of the number of active source messages accepted by the device).</td>
</tr>
<tr>
<td>Active source log-interval</td>
<td>Time (in seconds) between consecutive log messages on this peer.</td>
</tr>
</tbody>
</table>
Table 91: show msdp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keepalive messages sent</td>
<td>Number of keepalive messages sent.</td>
</tr>
<tr>
<td>Keepalive messages received</td>
<td>Number of keepalive messages received.</td>
</tr>
<tr>
<td>Unknown messages received</td>
<td>Number of unknown messages received.</td>
</tr>
<tr>
<td>Error messages received</td>
<td>Number of error messages received.</td>
</tr>
</tbody>
</table>

Sample Output

show msdp statistics

user@host> show msdp statistics
Global active source limit exceeded: 0
Global active source limit maximum: 10
Global active source limit threshold: 8
Global active source limit log-warn: 60
Global active source limit log-interval: 60

Peer: 10.255.245.39
Last State Change: 11:54:49 (00:24:59)
Last message received from peer: 11:53:32 (00:26:16)
RPF Failures: 0
Remote Closes: 0
Peer Timeouts: 0
SA messages sent: 376
SA messages received: 459
SA messages with zero Entry Count received: 0
SA request messages sent: 0
SA request messages received: 0
SA response messages sent: 0
SA response messages received: 0
Active source exceeded: 0
Active source Maximum: 10
Active source threshold: 8
Active source log-warn: 60
Active source log-interval: 120
Keepalive messages sent: 17
Keepalive messages received: 19
Unknown messages received: 0
Error messages received: 0

show msdp statistics peer

user@host> show msdp statistics peer 10.255.182.140
Peer: 10.255.182.140
Last State Change: 8:19:23 (00:01:08)
Last message received from peer: 8:20:05 (00:00:26)
RPF Failures: 0
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Closes</td>
<td>0</td>
</tr>
<tr>
<td>Peer Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>SA messages sent</td>
<td>17</td>
</tr>
<tr>
<td>SA messages received</td>
<td>16</td>
</tr>
<tr>
<td>SA request messages sent</td>
<td>0</td>
</tr>
<tr>
<td>SA request messages received</td>
<td>0</td>
</tr>
<tr>
<td>SA response messages sent</td>
<td>0</td>
</tr>
<tr>
<td>SA response messages received</td>
<td>0</td>
</tr>
<tr>
<td>Active source exceeded</td>
<td>20</td>
</tr>
<tr>
<td>Active source Maximum</td>
<td>10</td>
</tr>
<tr>
<td>Active source threshold</td>
<td>8</td>
</tr>
<tr>
<td>Active source log-warning</td>
<td>60</td>
</tr>
<tr>
<td>Active source log-interval</td>
<td>120</td>
</tr>
<tr>
<td>Keepalive messages sent</td>
<td>0</td>
</tr>
<tr>
<td>Keepalive messages received</td>
<td>0</td>
</tr>
<tr>
<td>Unknown messages received</td>
<td>0</td>
</tr>
<tr>
<td>Error messages received</td>
<td>0</td>
</tr>
</tbody>
</table>
**show multicast backup-pe-groups**

**Syntax**

```
show multicast backup-pe-groups
<address pe-address>
<group group-name>
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced in Junos OS Release 9.0.

**Description**

Display backup PE router group information when ingress PE redundancy is configured. Ingress PE redundancy provides a backup resource when point-to-multipoint LSPs are configured for multicast distribution.

**Options**

- none—Display standard information about all backup PE groups.
- address pe-address—(Optional) Display the groups that a PE address is associated with.
- group group—(Optional) Display the backup PE group information for a particular group.
- instance instance-name—(Optional) Display backup PE group information for a specific multicast instance.
- 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 multicast backup-pe-groups on page 1901

**Output Fields**

Table 92 on page 1900 describes the output fields for the `show multicast backup-pe-groups` command. Output fields are listed in the approximate order in which they appear.

*Table 92: show multicast backup-pe-groups Output Fields*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup PE Group</td>
<td>Group name.</td>
</tr>
<tr>
<td>Designated PE</td>
<td>Primary PE router. Address of the PE router that is currently forwarding traffic on the static route.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Number of times that the designated PE router has transitioned from the most eligible PE router to a backup PE router and back again to the most eligible PE router.</td>
</tr>
<tr>
<td>Last Transition</td>
<td>Time of the most recent transition.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Address of the local PE router.</td>
</tr>
</tbody>
</table>
Table 92: `show multicast backup-pe-groups` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup PE List</td>
<td>List of PE routers that are configured to be backups for the group.</td>
</tr>
</tbody>
</table>

Sample Output

```
show multicast backup-pe-groups

user@host> show multicast backup-pe-groups

Instance: master

Backup PE group: b1
  Designated PE: 10.255.165.7
  Transitions: 1
  Last Transition: 03:15:01
  Local Address: 10.255.165.7
  Backup PE List:
      10.255.165.8

Backup PE group: b2
  Designated PE: 10.255.165.7
  Transitions: 2
  Last Transition: 02:58:20
  Local Address: 10.255.165.7
  Backup PE List:
      10.255.165.9
      10.255.165.8
```
show multicast flow-map

List of Syntax  Syntax on page 1902
               Syntax (EX Series Switch and the QFX Series) on page 1902

Syntax        show multicast flow-map
               <brief | detail>
               <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)  show multicast flow-map
                                              <brief | detail>

Release Information  Command introduced in Junos OS Release 8.2.
                      Command introduced in Junos OS Release 9.0 for EX Series switches.
                      Command introduced in Junos OS Release 11.3 for the QFX Series.
                      Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Display configuration information about IP multicast flow maps.

Options
             none—Display configuration information about IP multicast flow maps on all systems.
             brief | detail—(Optional) Display the specified level of output.
             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 multicast flow-map on page 1903
                       show multicast flow-map detail on page 1903

Output Fields  Table 93 on page 1902 describes the output fields for the show multicast flow-map
               command. Output fields are listed in the approximate order in which they appear.

Table 93: show multicast flow-map Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Levels of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Policy</td>
<td>Name of the policy associated with the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Cache-timeout</td>
<td>Cache timeout value assigned to the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Bandwidth setting associated with the flow map.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 93: show multicast flow-map Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Levels of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive</td>
<td>Whether or not adaptive mode is enabled for the flow map.</td>
<td>none</td>
</tr>
<tr>
<td>Flow-map</td>
<td>Name of the flow map.</td>
<td>detail</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Whether or not adaptive mode is enabled for the flow map.</td>
<td>detail</td>
</tr>
<tr>
<td>Redundant Sources</td>
<td>Redundant sources defined for the same destination group.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show multicast flow-map

```
user@host> show multicast flow-map

Instance: master
Name  Policy                  Cache timeout  Bandwidth  Adaptive
map2  policy2                 never          2000000    no
map1  policy1                 60 seconds    2000000    no
```

Sample Output

show multicast flow-map detail

```
user@host> show multicast flow-map detail

Instance: master
Flow-map: map1
Policy: policy1
Cache Timeout: 600 seconds
Bandwidth: 2000000
Adaptive Bandwidth: yes
Redundant Sources: 10.11.11.11
Redundant Sources: 10.11.11.12
Redundant Sources: 10.11.11.13
```
**show multicast forwarding-cache statistics**

**Syntax**
```
show multicast forwarding-cache statistics
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Release Information**
Command introduced in Junos OS Release 12.2.
Starting in Junos OS Release 16.1, output includes general and rendezvous-point tree (RPT) suppression states.

**Description**
Display IP multicast forwarding cache statistics.

**Options**
- **none**—Display multicast forwarding cache statistics for all supported address families for all routing instances.
- **inet | inet6**—(Optional) Display multicast forwarding cache statistics for IPv4 or IPv6 family addresses, respectively.
- **instance instance-name**—(Optional) Display multicast forwarding cache statistics for a specific routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**Related Documentation**
- clear multicast forwarding-cache on page 1809
- threshold

**List of Sample Output**
- show multicast forwarding cache statistics instance on page 1905
- show multicast forwarding cache statistics instance (Forwarding-cache suppression is disabled) on page 1905

**Output Fields**
Table 94 on page 1904 describes the output fields for the `show multicast forwarding-cache statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 94: show multicast forwarding-cache statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance</strong></td>
<td>Name of the routing instance for which multicast forwarding cache statistics are displayed.</td>
</tr>
<tr>
<td><strong>Family</strong></td>
<td>Protocol family for which multicast forwarding cache statistics are displayed: ALL, INET, or INET6.</td>
</tr>
</tbody>
</table>
Table 94: show multicast forwarding-cache statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General (or MVPN RPT)</td>
<td></td>
</tr>
<tr>
<td>Suppression Active</td>
<td>Indicates whether suppression is configured.</td>
</tr>
<tr>
<td>General (or MVPN RPT)</td>
<td></td>
</tr>
<tr>
<td>Entries Used</td>
<td>Number of currently used multicast forwarding cache entries.</td>
</tr>
<tr>
<td>General (or MVPN RPT)</td>
<td></td>
</tr>
<tr>
<td>Suppress Threshold</td>
<td>Maximum number of multicast forwarding cache entries that can be added to the</td>
</tr>
<tr>
<td></td>
<td>cache. When the number of entries reaches the configured threshold, the device</td>
</tr>
<tr>
<td></td>
<td>suspends adding new multicast forwarding cache entries.</td>
</tr>
<tr>
<td>General (or MVPN RPT)</td>
<td></td>
</tr>
<tr>
<td>Reuse Value</td>
<td>Number of multicast forwarding cache entries that must be reached before the</td>
</tr>
<tr>
<td></td>
<td>device creates new multicast forwarding cache entries. When the total number of</td>
</tr>
<tr>
<td></td>
<td>multicast forwarding cache entries is below the reuse value, the device resumes</td>
</tr>
<tr>
<td></td>
<td>adding new multicast forwarding cache entries.</td>
</tr>
</tbody>
</table>

Sample Output

show multicast forwarding cache statistics instance

```
user@host> show multicast forwarding-cache statistic instance mvpn1 intet6
```

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance: mvpn1 Family:</td>
<td>INET6</td>
</tr>
<tr>
<td>General Suppression Active</td>
<td>Yes</td>
</tr>
<tr>
<td>General Entries Used</td>
<td>0</td>
</tr>
<tr>
<td>General Suppress Threshold</td>
<td>200</td>
</tr>
<tr>
<td>General Reuse Value</td>
<td>200</td>
</tr>
<tr>
<td>MVPN RPT Suppression Active</td>
<td>Yes</td>
</tr>
<tr>
<td>MVPN RPT Entries Used</td>
<td>0</td>
</tr>
<tr>
<td>MVPN RPT Suppress Threshold</td>
<td>200</td>
</tr>
<tr>
<td>MVPN RPT Reuse Value</td>
<td>200</td>
</tr>
</tbody>
</table>

show multicast forwarding cache statistics instance (Forwarding-cache suppression is disabled)

```
user@host> show multicast forwarding-cache statistic instance mvpn1
```

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance: mvpn1 Family:</td>
<td>ALL</td>
</tr>
<tr>
<td>Forwarding-cache suppression disabled Not enabled by configuration</td>
<td></td>
</tr>
</tbody>
</table>
show multicast interface

**List of Syntax**
- Syntax on page 1906
- Syntax (EX Series Switch and the QFX Series) on page 1906

**Syntax**
```
show multicast interface
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**
```
show multicast interface
```

**Release Information**
- Command introduced in Junos OS Release 8.3.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display bandwidth information about IP multicast interfaces.

**Options**
- none—Display all interfaces that have multicast configured.
- 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 multicast interface on page 1907

**Output Fields**
Table 95 on page 1906 describes the output fields for the `show multicast interface` command. Output fields are listed in the approximate order in which they appear.

**Table 95: show multicast interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the multicast interface.</td>
</tr>
<tr>
<td>Maximum bandwidth (bps)</td>
<td>Maximum bandwidth, in bits per second, for this interface.</td>
</tr>
<tr>
<td>Remaining bandwidth (bps)</td>
<td>Amount of bandwidth, in bits per second, remaining on the interface.</td>
</tr>
</tbody>
</table>
Table 95: show multicast interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Mapped bandwidth deduction (bps) | Amount of bandwidth, in bits per second, used by any flows that are mapped to the interface.  

**NOTE:** Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.  

This field does not appear in the output when the no QoS adjustment feature is disabled.

| Local bandwidth deduction (bps) | Amount of bandwidth, in bits per second, used by any mapped flows that are traversing the interface.  

**NOTE:** Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.  

This field does not appear in the output when the no QoS adjustment feature is disabled.

| Reverse OIF mapping | State of the reverse OIF mapping feature (on or off).  

**NOTE:** This field does not appear in the output when the no QoS adjustment feature is disabled.

| Reverse OIF mapping no QoS adjustment | State of the no QoS adjustment feature (on or off) for interfaces that are using reverse OIF mapping.  

**NOTE:** This field does not appear in the output when the no QoS adjustment feature is disabled.

| Leave timer | Amount of time a mapped interface remains active after the last mapping ends.  

**NOTE:** This field does not appear in the output when the no QoS adjustment feature is disabled.

| No QoS adjustment | State (on) of the no QoS adjustment feature when this feature is enabled.  

**NOTE:** This field does not appear in the output when the no QoS adjustment feature is disabled.

Sample Output

show multicast interface

```
user@host> show multicast interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Maximum bandwidth (bps)</th>
<th>Remaining bandwidth (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/3</td>
<td>10000000</td>
<td>0</td>
</tr>
<tr>
<td>fe-0/0/3.210</td>
<td>10000000</td>
<td>-2000000</td>
</tr>
<tr>
<td>fe-0/0/3.220</td>
<td>10000000</td>
<td>100000000</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Speed</th>
<th>Duplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/3.230</td>
<td></td>
<td>20000000</td>
<td></td>
</tr>
<tr>
<td>fe-0/0/2.200</td>
<td></td>
<td>100000000</td>
<td></td>
</tr>
</tbody>
</table>

*Interfaces Fundamentals for Routing Devices*
show multicast mrinfo

Syntax

show multicast mrinfo

<host>

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display configuration information about IP multicast networks, including neighboring multicast router addresses.

Options

none—Display configuration information about all multicast networks.

host—(Optional) Display configuration information about a particular host. Replace host with a hostname or IP address.

Required Privilege Level

view

List of Sample Output

show multicast mrinfo on page 1910

Output Fields

Table 96 on page 1909 describes the output fields for the show multicast mrinfo command. Output fields are listed in the approximate order in which they appear.

Table 96: show multicast mrinfo Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-address</td>
<td>Query address, hostname (DNS name or IP address of the source address), and multicast protocol version or the software version of another vendor.</td>
</tr>
<tr>
<td>ip-address-1→ip-address-2</td>
<td>Queried router interface address and directly attached neighbor interface address, respectively.</td>
</tr>
<tr>
<td>(name or ip-address)</td>
<td>Name or IP address of neighbor.</td>
</tr>
<tr>
<td>[metric/threshold/type/flags]</td>
<td>Neighbor’s multicast profile:</td>
</tr>
<tr>
<td></td>
<td>• metric—Always has a value of 1, because mrinfo queries the directly connected interfaces of a device.</td>
</tr>
<tr>
<td></td>
<td>• threshold—Multicast threshold time-to-live (TTL). The range of values is 0 through 255.</td>
</tr>
<tr>
<td></td>
<td>• type—Multicast connection type: pim or tunnel.</td>
</tr>
<tr>
<td></td>
<td>• flags—Flags for this route:</td>
</tr>
<tr>
<td></td>
<td>• querier—Queried router is the designated router for the neighboring session.</td>
</tr>
<tr>
<td></td>
<td>• leaf—Link is a leaf in the multicast network.</td>
</tr>
<tr>
<td></td>
<td>• down—Link status indicator.</td>
</tr>
</tbody>
</table>
Sample Output

code

```
show multicast mrinfo 10.35.4.1
```

```
user@host> show multicast mrinfo 10.35.4.1

10.35.4.1 (10.35.4.1) [version 12.0]:
192.168.195.166 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
10.38.20.1 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
10.47.1.1 -> 10.47.1.2 (10.47.1.2) [1/5/pim]
0.0.0.0 -> 0.0.0.0 (local) [1/0/pim/down]
```
**show multicast next-hops**

**List of Syntax**
- Syntax on page 1911
- Syntax (EX Series Switch and the QFX Series) on page 1911

**Syntax**
```
show multicast next-hops
  <brief | detail | terse>
  <identifier-number>
  <inet | inet6>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**
```
show multicast next-hops
  <brief | detail>
  <identifier-number>
  <inet | inet6>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `inet6` option introduced in Junos OS Release 10.0 for EX Series switches.
- `detail` option display of next-hop ID number introduced in Junos OS Release 11.1 for M Series and T Series routers and EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Support for bidirectional PIM added in Junos OS Release 12.1.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
- `terse` option introduced in Junos OS Release 16.1 for the MX Series.

**Description**
Display the entries in the IP multicast next-hop table.

**Options**
- `none`—Display standard information about all entries in the multicast next-hop table for all supported address families.
- `brief | detail | terse`—(Optional) Display the specified level of output. Use `terse` to display the total number of outgoing interfaces (as opposed to listing them). When you include the `detail` option on M Series and T Series routers and EX Series switches, the downstream interface name includes the next-hop ID number in parentheses, in the form `fe-0/1/2.0-(1048574)`, where `1048574` is the next-hop ID number.

Starting in Junos OS release 16.1, the `show multicast next-hops` statement shows the hierarchical next hops contained in the top-level next hop.

- `identifier-number`—(Optional) Show a particular next hop by ID number. The range of values is 1 through 65,535.
- `inet | inet6`—(Optional) Display entries for IPv4 or IPv6 family addresses, respectively.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level

List of Sample Output

- show multicast next-hops on page 1912
- show multicast next-hops (Ingress Router, Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 1912
- show multicast next-hops (Egress Router, Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 1913
- show multicast next-hops (Bidirectional PIM) on page 1913
- show multicast next-hops brief on page 1913
- show multicast next-hops detail on page 1913
- show multicast next-hops detail (PIM using point-to-multipoint mode) on page 1914

Output Fields

Table 97 on page 1912 describes the output fields for the show multicast next-hops command. Output fields are listed in the approximate order in which they appear.

**Table 97: show multicast next-hops Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
<td>Protocol family (such as INET).</td>
</tr>
<tr>
<td>ID</td>
<td>Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of cache entries that are using this next hop.</td>
</tr>
<tr>
<td>KRefcount</td>
<td>Kernel reference count for the next hop.</td>
</tr>
<tr>
<td>Downstream interface</td>
<td>Interface names associated with each multicast next-hop ID.</td>
</tr>
<tr>
<td>Incoming interface list</td>
<td>List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
</tr>
</tbody>
</table>

Sample Output

**show multicast next-hops**

```
user@host> show multicast next-hops
Family: INET
ID  Refcount  KRefcount  Downstream interface
262142  4        2          so-1/0/0.0
262143  2        1          mt-1/1/0.49152
262148  2        1          mt-1/1/0.32769
```

**show multicast next-hops (Ingress Router, Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)**

```
user@host> show multicast next-hops
Family: INET
ID  Refcount  KRefcount  Downstream interface  Addr
262142  4        2          so-1/0/0.0
262143  2        1          mt-1/1/0.49152
262148  2        1          mt-1/1/0.32769
```
show multicast next-hops (Egress Router, Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```
user@host> show multicast next-hops
Family: INET
ID     Refcount KRefcount Downstream interface     Addr
(0x600e844)  8     0    1048575
1048575    16    0 distributed-gmp
```

show multicast next-hops (Bidirectional PIM)

```
user@host> show multicast next-hops
Family: INET
ID     Refcount KRefcount Downstream interface
2097151    8     4    ge-0/0/1.0

Family: INET6
ID     Refcount KRefcount Downstream interface
2097157    2     1    ge-0/0/1.0

Family: Incoming interface list
ID     Refcount KRefcount Downstream interface
513     5     2    lo0.0
514     5     2    lo0.0
515     3     1    lo0.0
544     1     0    lo0.0
```

show multicast next-hops brief

The output for the `show multicast next-hops brief` command is identical to that for the `show multicast next-hops` command. For sample output, see `show multicast next-hops` on page 1912.

show multicast next-hops detail

```
user@host> show multicast next-hops detail
```
### show multicast next-hops detail (PIM using point-to-multipoint mode)

```bash
user@host> show multicast next-hops detail
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Refcount</th>
<th>KRefcount</th>
<th>Downstream interface</th>
<th>Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>262142</td>
<td>2</td>
<td>1</td>
<td>st0.0-192.0.2.0</td>
<td>0(573)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0-198.51.100.0(572)</td>
</tr>
</tbody>
</table>
show multicast pim-to-igmp-proxy

List of Syntax  Syntax on page 1915
               Syntax (EX Series Switch and the QFX Series) on page 1915

Syntax  

show multicast pim-to-igmp-proxy
       <instance instance-name>
       <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)

show multicast pim-to-igmp-proxy
       <instance instance-name>

Release Information

Command introduced in Junos OS Release 9.6 for EX Series switches.
instance option introduced in Junos OS Release 10.3.
instance option introduced in Junos OS Release 10.3 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display configuration information about PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy.

Options

none—Display configuration information about PIM-to-IGMP message translation for all routing instances.

instance instance-name—(Optional) Display configuration information about PIM-to-IGMP message translation for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

Level  view

Related Documentation

• Configuring PIM-to-IGMP and PIM-to-MLD Message Translation

List of Sample Output

show multicast pim-to-igmp-proxy on page 1916
show multicast pim-to-igmp-proxy instance on page 1916

Output Fields

Table 98 on page 1916 describes the output fields for the show multicast pim-to-igmp-proxy command. Output fields are listed in the order in which they appear.
Table 98: show multicast pim-to-igmp-proxy Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Routing instance. Default instance is master (inet.0 routing table).</td>
</tr>
<tr>
<td>Proxy state</td>
<td>State of PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy, on the configured upstream interfaces: enabled or disabled.</td>
</tr>
<tr>
<td>interface-name</td>
<td>Name of upstream interface (no more than two allowed) on which PIM-to-IGMP message translation is configured.</td>
</tr>
</tbody>
</table>

Sample Output

show multicast pim-to-igmp-proxy

```plaintext
user@host> show multicast pim-to-igmp-proxy
Instance: master Proxy state: enabled
  ge-0/1/0.1
  ge-0/1/0.2
```

show multicast pim-to-igmp-proxy instance

```plaintext
user@host> show multicast pim-to-igmp-proxy instance VPN-A
Instance: VPN-A Proxy state: enabled
  ge-0/1/0.1
```
show multicast pim-to-mld-proxy

List of Syntax
Syntax on page 1917
Syntax (EX Series Switch and the QFX Series) on page 1917

Syntax
show multicast pim-to-mld-proxy
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)
show multicast pim-to-mld-proxy
<instance instance-name>

Release Information
Command introduced in Junos OS Release 9.6 for EX Series switches.
instance option introduced in Junos OS Release 10.3.
instance option introduced in Junos OS Release 10.3 for EX Series switches.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display configuration information about PIM-to-MLD message translation, also known as PIM-to-MLD proxy.

Options
none—Display configuration information about PIM-to-MLD message translation for all routing instances.

instance instance-name—(Optional) Display configuration information about PIM-to-MLD message translation for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

List of Sample Output
show multicast pim-to-mld-proxy on page 1918
show multicast pim-to-mld-proxy instance on page 1918

Output Fields
Table 99 on page 1917 describes the output fields for the show multicast pim-to-mld-proxy command. Output fields are listed in the order in which they appear.

Table 99: show multicast pim-to-mld-proxy Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy state</td>
<td>State of PIM-to-MLD message translation, also known as PIM-to-MLD proxy, on the configured upstream interfaces: enabled or disabled.</td>
</tr>
</tbody>
</table>
Table 99: show multicast pim-to-mld-proxy Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>Name of upstream interface (no more than two allowed) on which PIM-to-MLD message translation is configured.</td>
</tr>
</tbody>
</table>

Sample Output

show multicast pim-to-mld-proxy

```
user@host> show multicast pim-to-mld-proxy
Instance: master Proxy state: enabled
ge-0/5/0.1
ge-0/5/0.2
```

show multicast pim-to-mld-proxy instance

```
user@host> show multicast pim-to-mld-proxy instance VPN-A
Instance: VPN-A Proxy state: enabled
ge-0/5/0.1
```
show multicast route

List of Syntax

Syntax

show multicast route
  <brief | detail | extensive | summary>
  <active | all | inactive>
  <group group>
  <inet | inet6>
  <instance instance name>
  <logical-system (all | logical-system-name)>
  <oif-count>
  <regular-expression>
  <source-prefix source-prefix>

Syntax (EX Series Switch and the QFX Series)

show multicast route
  <brief | detail | extensive | summary>
  <active | all | inactive>
  <group group>
  <inet | inet6>
  <instance instance name>
  <regular-expression>
  <source-prefix source-prefix>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
<oif-count> option introduced in Junos OS Release 16.1 for the MX Series.
Support for PIM NSR support for VXLAN added in Junos OS Release 16.2.
Support for multicast traffic counters added in Junos OS 19.2R1 for EX4300 switches.

Description

Display the entries in the IP multicast forwarding table. You can display similar information with the show route table inet.1 command.

NOTE: On all SRX Series devices, when a multicast route is not available, pending sessions are not torn down, and subsequent packets are queued. If no multicast route resolve comes back, then the traffic flow has to wait for the pending session to timed out. Then packets can trigger new pending session create and route resolve.
### Options

- **none**—Display standard information about all entries in the multicast forwarding table for all routing instances.
- **brief | detail | extensive | summary**—(Optional) Display the specified level of output.
- **active | all | inactive**—(Optional) Display all active entries, all entries, or all inactive entries, respectively, in the multicast forwarding table.
- **group group**—(Optional) Display the cache entries for a particular group.
- **inet | inet6**—(Optional) Display multicast forwarding table entries for IPv4 or IPv6 family addresses, respectively.
- **instance instance-name**—(Optional) Display entries in the multicast forwarding table for a specific multicast instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **oif-count**—(Optional) Display a count of outgoing interfaces rather than listing them.
- **regular-expression**—(Optional) Display information about the multicast forwarding table entries that match a UNIX OS-style regular expression.
- **source-prefix source-prefix**—(Optional) Display the cache entries for a particular source prefix.

### Required Privilege Level

**view**

### Related Documentation

- *Example: Configuring Multicast-Only Fast Reroute in a PIM Domain*

### List of Sample Output

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show multicast route</td>
<td>1922</td>
</tr>
<tr>
<td>show multicast route (Bidirectional PIM)</td>
<td>1923</td>
</tr>
<tr>
<td>show multicast route brief</td>
<td>1923</td>
</tr>
<tr>
<td>show multicast route summary</td>
<td>1923</td>
</tr>
<tr>
<td>show multicast route detail</td>
<td>1924</td>
</tr>
<tr>
<td>show multicast route extensive (Bidirectional PIM)</td>
<td>1924</td>
</tr>
<tr>
<td>show multicast route extensive (PIM using point-to-multipoint mode)</td>
<td>1925</td>
</tr>
<tr>
<td>show multicast route extensive (traffic counters)</td>
<td>1925</td>
</tr>
<tr>
<td>show multicast route instance &lt;instance-name&gt; extensive</td>
<td>1926</td>
</tr>
<tr>
<td>show multicast route extensive (PIM NSR support for VXLAN on master Routing Engine)</td>
<td>1927</td>
</tr>
<tr>
<td>show multicast route extensive (PIM NSR support for VXLAN on backup Routing Engine)</td>
<td>1927</td>
</tr>
<tr>
<td>show multicast route extensive (PIM NSR support for VXLAN on backup Routing Engine)</td>
<td>1928</td>
</tr>
<tr>
<td>show multicast route extensive (Junos OS Evolved)</td>
<td>1929</td>
</tr>
</tbody>
</table>
**Output Fields**  Table 100 on page 1921 describes the output fields for the **show multicastroute** 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>Instance</td>
<td>Name of the routing instance.</td>
<td>summary extensive</td>
</tr>
<tr>
<td>family</td>
<td>IPv4 address family (<strong>INET</strong>) or IPv6 address family (<strong>INET6</strong>).</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Prefix and length of the source as it is in the multicast forwarding table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Incoming interface list</td>
<td>List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
<td>All levels</td>
</tr>
<tr>
<td>Upstream interface</td>
<td>Name of the interface on which the packet with this source prefix is expected to arrive.</td>
<td>All levels</td>
</tr>
<tr>
<td>Upstream rpf interface list</td>
<td>When multicast-only fast reroute (MoFRR) is enabled, a PIM router propagates join messages on two upstream RPF interfaces to receive multicast traffic on both links for the same join request.</td>
<td>All levels</td>
</tr>
<tr>
<td>Downstream interface list</td>
<td>List of interface names to which the packet with this source prefix is forwarded.</td>
<td>All levels</td>
</tr>
<tr>
<td>Number of outgoing interfaces</td>
<td>Total number of outgoing interfaces for each (S,G) entry.</td>
<td>extensive</td>
</tr>
<tr>
<td>Session description</td>
<td>Name of the multicast session.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Statistics</td>
<td>Rate at which packets are being forwarded for this source and group entry (in Kbps and pps), and number of packets that have been forwarded to this prefix. If one or more of the kilobits per second packet forwarding statistic queries fails or times out, the statistics field displays <strong>Forwarding statistics are not available</strong>. <strong>NOTE:</strong> On QFX Series switches and OCX Series switches, this field does not report valid statistics.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Next-hop ID</td>
<td>Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine and is also displayed in the output of the <strong>show multicast nexthops</strong> command.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Incoming interface list ID</td>
<td>For bidirectional PIM, incoming interface list identifier. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 100: show multicast route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream protocol</td>
<td>The protocol that maintains the active multicast forwarding route for this group or source.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route type</td>
<td>Type of multicast route. Values can be (S,G) or (*,G).</td>
<td>summary</td>
</tr>
<tr>
<td>Route state</td>
<td>Whether the group is Active or Inactive.</td>
<td>summary extensive</td>
</tr>
<tr>
<td>Route count</td>
<td>Number of multicast routes.</td>
<td>summary</td>
</tr>
<tr>
<td>Forwarding state</td>
<td>Whether the prefix is pruned or forwarding.</td>
<td>extensive</td>
</tr>
<tr>
<td>Cache lifetime/timeout</td>
<td>Number of seconds until the prefix is removed from the multicast forwarding table.</td>
<td>extensive</td>
</tr>
<tr>
<td>Wrong incoming interface notifications</td>
<td>Number of times that the upstream interface was not available.</td>
<td>extensive</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time since the creation of a multicast route.</td>
<td>extensive</td>
</tr>
<tr>
<td>Sensor ID</td>
<td>Sensor ID corresponding to multicast route.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

Starting in Junos OS Release 16.1, show multicast route displays the top-level hierarchical next hop.

show multicast route

```
user@host> show multicast route
Family: INET

Group: 233.252.0.0
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0

Group: 233.252.0.1
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0
```
show multicast route (Bidirectional PIM)

user@host> show multicast route

Family: INET

Group: 233.252.0.1/24
Source: *
Incoming interface list:
  lo0.0 ge-0/0/1.0
Downstream interface list:
  ge-0/0/1.0

Group: 233.252.0.3/24
Source: *
Incoming interface list:
  lo0.0 ge-0/0/1.0 xe-4/1/0.0
Downstream interface list:
  ge-0/0/1.0

Group: 233.252.0.11/24
Source: *
Incoming interface list:
  lo0.0 ge-0/0/1.0
Downstream interface list:
  ge-0/0/1.0

Group: 233.252.0.13/24
Source: *
Incoming interface list:
  lo0.0 ge-0/0/1.0 xe-4/1/0.0
Downstream interface list:
  ge-0/0/1.0

Family: INET6

show multicast route brief

The output for the `show multicast route brief` command is identical to that for the `show multicast route` command. For sample output, see `show multicast route on page 1922` or `show multicast route (Bidirectional PIM) on page 1923`.

show multicast route summary

user@host> show multicast route summary

Instance: master Family: INET

<table>
<thead>
<tr>
<th>Route type</th>
<th>Route state</th>
<th>Route count</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S,G)</td>
<td>Active</td>
<td>2</td>
</tr>
<tr>
<td>(S,G)</td>
<td>Inactive</td>
<td>3</td>
</tr>
</tbody>
</table>
**show multicast route detail**

```
user@host> show multicast route detail

Family: INET

Group: 233.252.0.0
  Source: 10.255.14.144/32
  Upstream interface: local
  Downstream interface list:
    so-1/0/0.0
  Session description: Unknown
  Statistics: 8 kbps, 100 pps, 45272 packets
  Next-hop ID: 262142
  Upstream protocol: PIM

Group: 233.252.0.1
  Source: 10.255.14.144/32
  Upstream interface: local
  Downstream interface list:
    so-1/0/0.0
  Session description: Administratively Scoped
  Statistics: 0 kbps, 0 pps, 13404 packets
  Next-hop ID: 262142
  Upstream protocol: PIM

Group: 233.252.0.1
  Source: 10.255.70.15/32
  Upstream interface: so-1/0/0.0
  Downstream interface list:
    mt-1/1/0.1081344
  Session description: Administratively Scoped
  Statistics: 46 kbps, 1000 pps, 921077 packets
  Next-hop ID: 262143
  Upstream protocol: PIM

Family: INET6
```

**show multicast route extensive (Bidirectional PIM)**

```
user@host> show multicast route extensive

Family: INET

Group: 233.252.0.1/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0
  Downstream interface list:
    ge-0/0/1.0
  Number of outgoing interfaces: 1
  Session description: NOB Cross media facilities
  Statistics: 0 kbps, 0 pps, 0 packets
  Next-hop ID: 2097153
  Incoming interface list ID: 585
```
show multicast route extensive (PIM using point-to-multipoint mode)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 225.0.0.1
Source: 192.0.2.0/24
Upstream interface: st0.1
+ Upstream neighbor: 203.0.113.0/24
Downstream interface list:
+ st0.0-198.51.100.0 st0.0-198.51.100.1
Session description: Unknown
Statistics: 0 kbps, 1pps, 119 packets
Next-hop ID: 262142
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: 360 seconds
Wrong incoming interface notifications: 0
Uptime: 00:02:00

show multicast route extensive (traffic counters)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 225.0.0.1
Source: 192.0.2.0/24
Upstream interface: ge-3/0/12.0
Downstream interface list:
  ge-0/0/18.0 ge-0/0/7.0 ge-2/0/11.0 ge-2/0/7.0 ge-3/0/20.0 ge-3/0/21.0
Number of outgoing interfaces: 6
Session description: Unknown
Statistics: 102 kBps, 801 pps, 5735 packets
Next-hop ID: 131076
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: 360 seconds
Wrong incoming interface notifications: 0
Uptime: 00:03:57

```
show multicast route instance <instance-name> extensive
```

```
user@host> show multicast route instance mvpn extensive
Family: INET
Group: 233.252.0.10
Source: 10.0.0.2/32
Upstream interface: xe-0/0/0.102
Downstream interface list:
  xe-10/3/0.0 xe-0/3/0.0 xe-0/0/0.106 xe-0/0/0.105
  xe-0/0/0.103 xe-0/0/0.104 xe-0/0/0.107 xe-0/0/0.108
Session description: Administratively Scoped
Statistics: 256 kBps, 3998 pps, 670150 packets
Next-hop ID: 1048579
Upstream protocol: MVPN
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 58
Uptime: 00:00:04

Instance: master Family: INET

Group: 225.0.0.1
Source: 101.0.0.2/32
Upstream interface: ge-2/2/0.101
Downstream interface list:
  distributed-gmp
Number of outgoing interfaces: 1
Session description: Unknown
Statistics: 105 kBps, 2500 pps, 4153361 packets
Next-hop ID: 1048575
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: 360 seconds
Wrong incoming interface notifications: 0
Uptime: 00:31:46

Group: 225.0.0.1
Source: 101.0.0.3/32
Upstream interface: ge-2/2/0.101
Downstream interface list:
  distributed-gmp
Number of outgoing interfaces: 1
Session description: Unknown
Statistics: 105 kBps, 2500 pps, 4153289 packets
Next-hop ID: 1048575
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: 360 seconds
Wrong incoming interface notifications: 0
Uptime: 00:31:46

show multicast route extensive (PIM NSR support for VXLAN on master Routing Engine)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 233.252.0.1
Source: 10.3.3.3/32
Upstream interface: ge-3/1/2.0
Downstream interface list:
-(593)
Number of outgoing interfaces: 1
Session description: Organisational Local Scope
Statistics: 0 kbps, 0 pps, 27 packets
Next-hop ID: 1048576
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding (Forwarding state is set as 'Forwarding' in master RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:06:38

Group: 233.252.0.1
Source: 10.2.1.4/32
Upstream interface: local
Downstream interface list: ge-3/1/2.0
Number of outgoing interfaces: 1
Session description: Organisational Local Scope
Statistics: 0 kbps, 0 pps, 86 packets
Next-hop ID: 1048575
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding (Forwarding state is set as 'Forwarding' in master RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:07:45

Instance: master Family: INET6

show multicast route extensive (PIM NSR support for VXLAN on backup Routing Engine)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 233.252.0.1
Source: 10.3.3.3/32
Upstream interface: ge-3/1/2.0
Number of outgoing interfaces: 0
Session description: Organisational Local Scope
Forwarding statistics are not available
Next-hop ID: 0
Upstream protocol: PIM
Route state: Active
Forwarding state: Pruned (Forwarding state is set as 'Pruned' in backup RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:06:46

Group: 233.252.0.1
Source: 10.2.1.4/32
Upstream interface: local
Number of outgoing interfaces: 0
Session description: Organisational Local Scope
Forwarding statistics are not available
Next-hop ID: 0
Upstream protocol: PIM
Route state: Active
Forwarding state: Pruned (Forwarding state is set as 'Pruned' in backup RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:07:54

Instance: master Family: INET6

show multicast route extensive (PIM NSR support for VXLAN on backup Routing Engine)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 233.252.0.1
Source: 10.3.3.3/32
Upstream interface: ge-3/1/2.0
Downstream interface list:
-(593)
Number of outgoing interfaces: 1
Session description: Organisational Local Scope
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 1048576
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding (Forwarding state is set as 'Forwarding' in backup RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:06:38

Group: 233.252.0.1
Source: 10.2.1.4/32
Upstream interface: local
Downstream interface list:
ge-3/1/2.0
Number of outgoing interfaces: 1
Session description: Organisational Local Scope
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 1048575
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding (Forwarding state is set as 'Forwarding' in backup RE.)
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 00:07:45

Instance: master Family: INET6

show multicast route extensive (Junos OS Evolved)

user@host> show multicast route extensive

Instance: master Family: INET

Group: 232.255.255.100
Source: 10.1.1.2/32
Upstream interface: et-0/0/0:0.0
Downstream interface list:
  et-0/0/2:1.0 et-0/0/1:0.0
Number of outgoing interfaces: 2
Session description: Source specific multicast
Statistics: 0 kBps, 0 pps, 0 packets
Next-hop ID: 11066
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0
Uptime: 14:58:34
Sensor ID: 0xf0000002
show multicast rpf

List of Syntax  Syntax on page 1930
Syntax (EX Series Switch and the QFX Series) on page 1930

Syntax
show multicast rpf

<inet | inet6>

<instance instance-name>
<logical-system (all | logical-system-name)>
<prefix>
<summary>

Syntax (EX Series Switch and the QFX Series)
show multicast rpf

<inet | inet6>

<instance instance-name>
<prefix>
<summary>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Display information about multicast reverse-path-forwarding (RPF) calculations.

Options
none—Display RPF calculation information for all supported address families.

inet | inet6—(Optional) Display the RPF calculation information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display information about multicast RPF calculations for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

prefix—(Optional) Display the RPF calculation information for the specified prefix.

summary—(Optional) Display a summary of all multicast RPF information.

Required Privilege
view

List of Sample Output
show multicast rpf on page 1931
show multicast rpf inet6 on page 1932
show multicast rpf prefix on page 1933
show multicast rpf summary on page 1933
Output Fields  

Table 101 on page 1931 describes the output fields for the `show multicast rpf` 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>Instance</td>
<td>Name of the routing instance. (Displayed when multicast is configured within a routing instance.)</td>
</tr>
<tr>
<td>Source prefix</td>
<td>Prefix and length of the source as it exists in the multicast forwarding table.</td>
</tr>
<tr>
<td>Protocol</td>
<td>How the route was learned.</td>
</tr>
<tr>
<td>Interface</td>
<td>Upstream RPF interface.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Upstream RPF neighbor.</td>
</tr>
</tbody>
</table>
```

NOTE: The displayed interface information does not apply to bidirectional PIM RP addresses. This is because the `show multicast rpf` command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF interface information, always use the `show pim join extensive` command when bidirectional PIM is configured.

NOTE: The displayed neighbor information does not apply to bidirectional PIM. This is because the `show multicast rpf` command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF neighbor information, always use the `show pim join extensive` command when bidirectional PIM is configured.

Sample Output

```
show multicast rpf

Multicast RPF table: inet.0, 12 entries

0.0.0.0/0
  Protocol: Static

10.255.14.132/32
  Protocol: Direct
  Interface: lo0.0

10.255.245.91/32
  Protocol: IS-IS
  Interface: so-1/1/1.0
  Neighbor: 192.168.195.21

172.16.0.1/32
  Inactive

172.16.0.0/12
  Protocol: Static
```
show multicast rpf inet6

user@host> show multicast rpf inet6

Multicast RPF table: inet6.0, 12 entries

::10.255.14.132/128  
    Protocol: Direct  
    Interface: lo0.0

::10.255.245.91/128  
    Protocol: IS-IS  
    Interface: so-1/1/1.0  
    Neighbor: 2001:db8::2a0:a5ff:fe28:2e8c

::192.168.195.20/126  
    Protocol: Direct  
    Interface: so-1/1/1.0

::192.168.195.22/128  
    Protocol: Local

::192.168.195.36/126  
    Protocol: IS-IS  
    Interface: so-1/1/1.0  
    Neighbor: 2001:db8::2a0:a5ff:fe28:2e8c

::192.168.195.76/126  
    Protocol: Direct  
    Interface: fe-2/2/0.0
show multicast rpf prefix

user@host> show multicast rpf 2001:db8::/16

Multicast RPF table: inet6.0, 13 entries

2001:db8::2/128
 Protocol: PIM

2001:db8::d/128
 Protocol: PIM

...

show multicast rpf summary

user@host> show multicast rpf summary

Multicast RPF table: inet.0, 16 entries
Multicast RPF table: inet6.0, 12 entries
**show multicast scope**

**List of Syntax**

Syntax on page 1934  
Syntax (EX Series Switch and the QFX Series) on page 1934

Syntax

```
show multicast scope
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
show multicast scope
<inet | inet6>
<instance instance-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display administratively scoped IP multicast information.

**Options**

`none`—Display standard information about administratively scoped multicast information for all supported address families in all routing instances.

`inet | inet6`—(Optional) Display scoped multicast information for IPv4 or IPv6 family addresses, respectively.

`instance instance-name`—(Optional) Display administratively scoped information for a specific multicast instance.

`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 multicast scope on page 1935  
show multicast scope inet on page 1935  
show multicast scope inet6 on page 1935

**Output Fields**

Table 102 on page 1935 describes the output fields for the `show multicast scope` command. Output fields are listed in the approximate order in which they appear.
Table 102: `show multicast scope` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope name</td>
<td>Name of the multicast scope.</td>
</tr>
<tr>
<td>Group Prefix</td>
<td>Range of multicast groups that are scoped.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that is the boundary of the administrative scope.</td>
</tr>
<tr>
<td>Resolve Rejects</td>
<td>Number of kernel resolve rejects.</td>
</tr>
</tbody>
</table>

Sample Output

`show multicast scope`

```
user@host> show multicast scope

<table>
<thead>
<tr>
<th>Scope name</th>
<th>Group Prefix</th>
<th>Interface</th>
<th>Resolve Rejects</th>
</tr>
</thead>
<tbody>
<tr>
<td>233-net</td>
<td>233.252.0.0/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>233.252.0.1/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>2001:db8::/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
<tr>
<td>larry</td>
<td>2001:db8::1234/128</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

`show multicast scope inet`

```
user@host> show multicast scope inet

<table>
<thead>
<tr>
<th>Scope name</th>
<th>Group Prefix</th>
<th>Interface</th>
<th>Resolve Rejects</th>
</tr>
</thead>
<tbody>
<tr>
<td>233-net</td>
<td>233.252.0.0/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>233.252.0.0/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

`show multicast scope inet6`

```
user@host> show multicast scope inet6

<table>
<thead>
<tr>
<th>Scope name</th>
<th>Group Prefix</th>
<th>Interface</th>
<th>Resolve Rejects</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>2001:db8::/16</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
<tr>
<td>larry</td>
<td>2001:db8::1234/128</td>
<td>fe-0/0/0.1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show multicast snooping next-hops

**Syntax**
```
show multicast snooping next-hops
  <brief | detail>
  <identifier next-hop-ID>
  <inet>
  <inet6>
  <logical-system logical-system-name>
```

**Release Information**
Command introduced in Junos OS Release 11.2.

**Description**
Display information about the IP multicast snooping next-hops.

**Options**
- `brief | detail`—(Optional) Display the specified level of output.
- `inet`—(Optional) Display information for IPv4 multicast next hops only. If a family is not specified, both IPv4 and IPv6 results will be shown.
- `inet6`—(Optional) Display information for IPv6 multicast next hops only. If a family is not specified, both IPv4 and IPv6 results will be shown.
- `logical-system logical-system-name`—(Optional) Display information about a particular logical system, or type 'all'.

**Required Privilege Level**
view

**List of Sample Output**
- show multicast snooping next-hops on page 1938
- show multicast snooping next-hops (IGMP snooping enabled on a VPLS) on page 1938

**Output Fields**
Table 103 on page 1936 describes the output fields for the `show multicast snooping next-hops` 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>Family</td>
<td>Protocol family for which multicast snooping next hops are displayed: INET or INET6.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of cache entries that are using this next hop.</td>
</tr>
<tr>
<td>KRefcount</td>
<td>Kernel reference count for the next hop.</td>
</tr>
<tr>
<td>Downstream interface</td>
<td>Interface names associated with each multicast next-hop ID.</td>
</tr>
</tbody>
</table>
### Table 103: show multicast snooping next-hops Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nexthop Id</strong></td>
<td>Identifier for the next-hop.</td>
</tr>
</tbody>
</table>

**NOTE:** To see the next-hop ID for a given PE mesh group, `igmp-snooping` must be enabled for the relevant VPLS routing instance. (Junos OS creates a default CE and VE mesh groups for each VPLS routing instance. The next hop of the VE mesh group is the set of VE mesh-group interfaces of the remaining PEs in the same VPLS routing instance.)
**Sample Output**

**show multicast snooping next-hops**

```
user@host> show multicast snooping next-hops

Family: INET
ID     Refcount KRefcount Downstream interface     Nexthop Id
1048574  4             1 ge-0/1/0.1000
ge-0/1/2.1000
ge-0/1/3.1000
1048574  4             1 ge-0/1/0.1000--(2000)
1048575  2             0 ge-0/1/2.1000--(2001)
ge-0/1/3.1000--(2002)
1048576  2             0 lsi.1048578--(2003)
lsi.1048579--(2004)
```

**show multicast snooping next-hops (IGMP snooping enabled on a VPLS)**

In this example, ID 1048585 is the VE next-hop ID created for the VE next hop that is holding VE interfaces for the routing instance. It only appears if igmp snooping is enabled on the VPLS.

```
user@host> show multicast snooping next-hops

Family: INET
ID     Refcount KRefcount Downstream interface     Addr
1048588  2             1 1048585
1048589  2             1 1048585
0        2             0 ge-0/0/1.100
ge-0/0/5.100
1048583  2             1 local
1048587  2             1 local
1048586  4             2 local
1048585
ge-0/0/5.100
1048584  2             1 local
ge-0/0/5.100
1048582  6             2 ge-0/0/5.100
0        2             0 ge-0/0/2.200
ge-0/0/0.200
0        2             0 ge-0/0/0.300
ge-0/0/2.300
0        1             0 vt-0/0/10.17825792
vt-0/0/10.17825793
0        1             0 vt-0/0/10.1048576
vt-0/0/10.1048578
1048585  5             0 vt-0/0/10.1048577
vt-0/0/10.1048579
0        1             0 vt-0/0/10.34603008
vt-0/0/10.34603009
```
show multicast sessions

List of Syntax  Syntax on page 1940
Syntax (EX Series Switch and the QFX Series) on page 1940

Syntax  show multicast sessions
        <brief | detail | extensive>
        <logical-system (all | logical-system-name)>
        <regular-expression>

Syntax (EX Series Switch and the QFX Series)  show multicast sessions
                                                <brief | detail | extensive>
                                                <regular-expression>

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 11.3 for the QFX Series.
                      Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Display information about announced IP multicast sessions.

NOTE: On all SRX Series devices, only 100 packets can be queued during pending (S, G) route. However, when multiple multicast sessions enter the route resolve process at the same time, buffer resources are not sufficient to queue 100 packets for each session.

Options  none—Display standard information about all multicast sessions for all routing instances.
        brief | detail | extensive—(Optional) Display the specified level of output.
        logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
        regular-expression—(Optional) Display information about announced sessions that match a UNIX-style regular expression.

Required Privilege  view

List of Sample Output  show multicast sessions on page 1942
                         show multicast sessions regular-expression detail on page 1942

Output Fields  Table 104 on page 1941 describes the output fields for the show multicast sessions command. Output fields are listed in the approximate order in which they appear.
### Table 104: show multicast sessions Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-name</td>
<td>Name of the known announced multicast sessions.</td>
</tr>
</tbody>
</table>
### Sample Output

**show multicast sessions**

```bash
callback> show multicast sessions
```

<table>
<thead>
<tr>
<th>1-Department of Biological Sciences, LSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monterey Bay - DockCam</td>
</tr>
<tr>
<td>Monterey Bay - JettyCam</td>
</tr>
<tr>
<td>Monterey Bay - StandCam</td>
</tr>
<tr>
<td>Monterey DockCam</td>
</tr>
<tr>
<td>Monterey DockCam / ROV cam</td>
</tr>
</tbody>
</table>

... | NASA TV (MPEG-1) |...

| UO Broadcast - NASA Videos - 25 Years of Progress |
| UO Broadcast - NASA Videos - Journey through the Solar System |
| UO Broadcast - NASA Videos - Life in the Universe |
| UO Broadcast - NASA Videos - Nasa and the Airplane |
| UO Broadcasts OPB's Oregon Story |
| UO DOD News Clips |
| UO Medical Management of Biological Casualties (1) |
| UO Medical Management of Biological Casualties (2) |
| UO Medical Management of Biological Casualties (3) |

... 376 active sessions.

**show multicast sessions regular-expression detail**

```bash
callback> show multicast sessions "NASA TV" detail
```

**SDP Version: 0**  **Originated by: -010.223.83.33**
**Description:** NASA television in MPEG-1 format, provided by Private University.
**Please contact the UO if you have problems with this feed.**
**Email:** Your Name Here <multicast@lists.private.edu>
**Phone:** Your Name Here <888/555-1212>
**Bandwidth:** AS:1000
**Start time:** permanent
**Stop time:** none
**Attribute:** type:broadcast
**Attribute:** tool:IP/TV Content Manager 3.4.14
**Attribute:** live:capture:1
**Attribute:** x-iptv-capture:mpls
**Media:** video 54302 RTP/AVP 32 31 96 97
**Connection Data:** 233.252.0.45 ttl 127
**Attribute:** quality:8
**Attribute:** framerate:30
**Attribute:** rtppmap:96 WBIH/90000
**Attribute:** rtppmap:97 MP4V-ES/90000
**Attribute:** x-iptv-srv:video 10.223.91.191 live
**Attribute:** fmsg:32 type=mpeg1
**Media:** audio 28848 RTP/AVP 14 0 96 3 5 97 98 99 100 101 102 10 11 103 104 105 106
**Connection Data:** 224.2.145.37 ttl 127
**Attribute:** rtppmap:96 X-WAVE/8000
**Attribute:** rtppmap:97 L8/8000/2
**Attribute:** rtppmap:98 L8/8000
**Attribute:** rtppmap:99 L8/22050/2
**Attribute:** rtppmap:100 L8/22050
Attribute: rtpmap:101 L8/11025/2
Attribute: rtpmap:102 L8/11025
Attribute: rtpmap:103 L16/22050/2
Attribute: rtpmap:104 L16/22050

1 matching sessions.
show multicast snooping route

Syntax

show multicast snooping route
<regexp>
<active>
<all>
<bridge-domain bridge-domain-name>
<brief>
<control>
<data>
<detail>
<extensive>
<group group>
<inactive>
/inet>
<inet6>
<instance instance-name>
<logical-system logical-system-name>
<mesh-group mesh-group-name>
<qualified-vlan vlan-id>
<source-prefix source-prefix>
<vlan vlan-id>

Release Information

Command introduced in Junos OS Release 8.5.
Support for control, data, qualified-vlan and vlan options introduced in Junos OS Release 13.3 for EX Series switches.

Description

Display the entries in the IP multicast snooping forwarding table. You can display some of this information with the show route table inet.1 command.

Options

none—Display standard information about all entries in the multicast snooping table for all virtual switches and all bridge domains.

active | all | inactive—(Optional) Display all active entries, all entries, or all inactive entries, respectively, in the multicast snooping table.

bridge-domain bridge-domain—(Optional) Display the entries for a particular bridge domain.

brief | detail | extensive—(Optional) Display the specified level of output.

control—(Optional) Display control route entries.

data—(Optional) Display data route entries.

group group—(Optional) Display the entries for a particular group.

inet—(Optional) Display IPv4 information.

inet6—(Optional) Display IPv6 information.
instance instance-name—(Optional) Display the entries for a multicast instance.

logical-system logical-system-name—(Optional) Display information about a particular logical system, or type 'all'.

mesh-group mesh-group-name—(Optional) Display the entries for a particular mesh group.

qualified-vlan vlan-id—(Optional) Display the entries for a particular qualified VLAN.

regexp—(Optional) Display information about the multicast forwarding table entries that match a UNIX-style regular expression.

source-prefix source-prefix—(Optional) Display the entries for a particular source prefix.

vlan vlan-id—(Optional) Display the entries for a particular VLAN.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
</tr>
</tbody>
</table>

**List of Sample Output**

- show multicast snooping route bridge-domain on page 1946
- show multicast snooping route instance vs on page 1946
- show multicast snooping route extensive on page 1946
- show multicast snooping route extensive group on page 1947

**Output Fields**

Table 105 on page 1945 describes the output fields for the show multicast snooping route command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th><strong>Table 105: show multicast snooping route Output Fields</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field Name</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Nexthop Bulking</td>
</tr>
<tr>
<td>Family</td>
</tr>
<tr>
<td>Group</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Routing-instance</td>
</tr>
<tr>
<td>Learning Domain</td>
</tr>
<tr>
<td>Statistics</td>
</tr>
<tr>
<td>Next-hop ID</td>
</tr>
</tbody>
</table>
Table 105: show multicast snooping route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route state</td>
<td>Whether the group is Active or Inactive.</td>
<td>extensive</td>
</tr>
<tr>
<td>Forwarding state</td>
<td>Whether the prefix is Pruned or Forwarding.</td>
<td>extensive</td>
</tr>
<tr>
<td>Cache lifetime/timeout</td>
<td>Number of seconds until the prefix is removed from the multicast forwarding table. A value of never indicates a permanent forwarding entry.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

**show multicast snooping route bridge-domain**

```plaintext
tabutt@host> show multicast snooping route bridge-domain br-dom-1 extensive
Family: INET
Group: 232.1.1.1
  Source: 192.168.3.100/32
  Downstream interface list:
    ge-0/1/0.200
  Statistics: 0 kbps, 0 pps, 1 packets
  Next-hop ID: 1048577
  Route state: Active
  Forwarding state: Forwarding
  Cache lifetime/timeout: 240 seconds
```

**show multicast snooping route instance vs**

```plaintext
tabutt@host> show multicast snooping route instance vs
Nexthop Bulking: ON
Family: INET
Group: 224.0.0.0
  Bridge-domain: vsid500
Group: 225.1.0.1
  Bridge-domain: vsid500
  Downstream interface list: vsid500
    ge-0/3/8.500 ge-1/1/9.500 ge1/2/5.500
```

**show multicast snooping route extensive**

```plaintext
tabutt@host> show multicast snooping route extensive inet6 group ff03::1
Nexthop Bulking: OFF
Family: INET6
Group: ff03::1/128
  Source: ::
  Bridge-domain: BD-1
  Mesh-group: __all_ces__
  Downstream interface list:
```
```
show multicast snooping route extensive group

user@host> show multicast snooping route extensive instance evpn-vxlan group 233.252.0.1/

Group: 233.252.0.1/32
Source: *
Vlan: VLAN-100
Mesh-group: __all_ces__
   Downstream interface list:
       ge-0/0/3.0 -(662)
       evpn-core-nh -(131076)
Statistics: 0 kBps, 0 pps, 0 packets
Next-hop ID: 131070
Route state: Active
Forwarding state: Forwarding
```

**show multicast statistics**

Syntax

```
show multicast statistics
/inet|/inet6>
(instance instance-name)>
(interface interface-name)>
(logical-system (all | logical-system-name)>
```

Release Information

Command introduced before Junos OS Release 7.4.
`interface` option introduced in Junos OS Release 16.1 for the MX Series.

Description

Display IP multicast statistics.

Options

- **none**—Display multicast statistics for all supported address families for all routing instances.
- **inet | inet6**—(Optional) Display multicast statistics for IPv4 or IPv6 family addresses, respectively.
- **instance instance-name**—(Optional) Display statistics for a specific routing instance.
- **interface interface-name**—(Optional) Display statistics for a specific interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Additional Information

The input and output interface multicast statistics are consistent, but not timely. They are constructed from the forwarding statistics, which are gathered at 30-second intervals. Therefore, the output from this command always lags the true count by up to 30 seconds.

Required Privilege

**view**

Related Documentation

- clear multicast statistics on page 1814

List of Sample Output

- show multicast statistics on page 1951
- show multicast statistics (PIM using point-to-multipoint mode) on page 1951
- show multicast statistics interface on page 1952

Output Fields

`Table 106 on page 1948` describes the output fields for the `show multicast statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 106: show multicast statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
</tbody>
</table>
Table 106: `show multicast statistics` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
<td>Protocol family for which multicast statistics are displayed: INET or INET6.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface for which statistics are being reported.</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Primary multicast protocol on the interface: PIM, DVMRP for INET, or PIM for INET6.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>Number of multicast packets that did not arrive on the correct upstream interface.</td>
</tr>
<tr>
<td>Kernel Resolve</td>
<td>Number of resolve requests processed by the primary multicast protocol on the interface.</td>
</tr>
<tr>
<td>Resolve No Route</td>
<td>Number of resolve requests that were ignored because there was no route to the source.</td>
</tr>
<tr>
<td>Resolve Filtered</td>
<td>Number of resolve requests filtered by policy if any policy is configured.</td>
</tr>
<tr>
<td>In Kbytes</td>
<td>Total accumulated incoming packets (in KB) since the last time the <code>clear multicast statistics</code> command was issued.</td>
</tr>
<tr>
<td>Out Kbytes</td>
<td>Total accumulated outgoing packets (in KB) since the last time the <code>clear multicast statistics</code> command was issued.</td>
</tr>
<tr>
<td>Mismatch error</td>
<td>Number of mismatches that were ignored because of internal errors.</td>
</tr>
<tr>
<td>Mismatch No Route</td>
<td>Number of mismatches that were ignored because there was no route to the source.</td>
</tr>
<tr>
<td>Routing Notify</td>
<td>Number of times that the multicast routing system has been notified of a new multicast source by a multicast routing protocol .</td>
</tr>
<tr>
<td>Resolve Error</td>
<td>Number of resolve requests that were ignored because of internal errors.</td>
</tr>
<tr>
<td>In Packets</td>
<td>Total number of incoming packets since the last time the <code>clear multicast statistics</code> command was issued.</td>
</tr>
<tr>
<td>Out Packets</td>
<td>Total number of outgoing packets since the last time the <code>clear multicast statistics</code> command was issued.</td>
</tr>
<tr>
<td>Resolve requests on interfaces not enabled for multicast n</td>
<td>Number of resolve requests on interfaces that are not enabled for multicast that have accumulated since the <code>clear multicast statistics</code> command was last issued.</td>
</tr>
<tr>
<td>Resolve requests with no route to source n</td>
<td>Number of resolve requests with no route to the source that have accumulated since the <code>clear multicast statistics</code> command was last issued.</td>
</tr>
<tr>
<td>Routing notifications on interfaces not enabled for multicast n</td>
<td>Number of routing notifications on interfaces not enabled for multicast that have accumulated since the <code>clear multicast statistics</code> command was last issued.</td>
</tr>
<tr>
<td>Routing notifications with no route to source n</td>
<td>Number of routing notifications with no route to the source that have accumulated since the <code>clear multicast statistics</code> command was last issued.</td>
</tr>
</tbody>
</table>
Table 106: show multicast statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Mismatches on interfaces not enabled for multicast</td>
<td>Number of interface mismatches on interfaces not enabled for multicast that have accumulated since the clear multicast statistics command was last issued.</td>
</tr>
<tr>
<td>Group Membership on interfaces not enabled for multicast</td>
<td>Number of group memberships on interfaces not enabled for multicast that have accumulated since the clear multicast statistics command was last issued.</td>
</tr>
</tbody>
</table>
Sample Output

show multicast statistics

<table>
<thead>
<tr>
<th>Address family: INET</th>
<th>Interface: fe-0/0/0</th>
<th>Routing Protocol: PIM</th>
<th>Mismatch error: 0</th>
<th>Mismatch: 0</th>
<th>Routing Notify: 0</th>
<th>Kernel Resolve: 10</th>
<th>Resolve No Route: 0</th>
<th>In Kbytes: 4641</th>
<th>Out Kbytes: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface: so-0/1/1.0</td>
<td>Routing Protocol: PIM</td>
<td>Mismatch error: 0</td>
<td>Mismatch: 0</td>
<td>Routing Notify: 0</td>
<td>Kernel Resolve: 0</td>
<td>Resolve No Route: 0</td>
<td>In Kbytes: 0</td>
<td>Out Kbytes: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Resolve requests on interfaces not enabled for multicast 0
Resolve requests with no route to source 0
Routing notifications on interfaces not enabled for multicast 0
Routing notifications with no route to source 0
Interface Mismatches on interfaces not enabled for multicast 0
Group Membership on interfaces not enabled for multicast 25

<table>
<thead>
<tr>
<th>Address family: INET6</th>
<th>Interface: fe-0/0/0.0</th>
<th>Routing Protocol: PIM</th>
<th>Mismatch error: 0</th>
<th>Mismatch: 0</th>
<th>Routing Notify: 0</th>
<th>Kernel Resolve: 0</th>
<th>Resolve No Route: 0</th>
<th>In Kbytes: 0</th>
<th>Out Kbytes: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interface: so-0/1/1.0</td>
<td>Routing Protocol: PIM</td>
<td>Mismatch error: 0</td>
<td>Mismatch: 0</td>
<td>Routing Notify: 0</td>
<td>Kernel Resolve: 0</td>
<td>Resolve No Route: 0</td>
<td>In Kbytes: 0</td>
<td>Out Kbytes: 0</td>
</tr>
</tbody>
</table>

Resolve requests on interfaces not enabled for multicast 0
Resolve requests with no route to source 0
Routing notifications on interfaces not enabled for multicast 0
Routing notifications with no route to source 0
Interface Mismatches on interfaces not enabled for multicast 0
Group Membership on interfaces not enabled for multicast 0

show multicast statistics (PIM using point-to-multipoint mode)

<table>
<thead>
<tr>
<th>Interface: st0.0-192.0.2.0</th>
<th>Routing protocol: PIM</th>
<th>Mismatch error: 0</th>
<th>Mismatch: 0</th>
<th>Routing notify: 0</th>
<th>Kernel resolve: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
show multicast statistics interface

user@host>  show multicast statistics interface vt-3/0/10.2097152

Instance: master Family: INET
Interface: vt-3/0/10.2097152
Routing protocol: PIM Mismatch error: 0
Mismatch: 0 Mismatch no route: 0
Kernel resolve: 0 Routing notify: 0
Resolve no route: 0 Resolve error: 0
Resolve filtered: 0 Notify filtered: 0
In kbytes: 0 In packets: 0
Out kbytes: 0 Out packets: 0
show multicast usage

**List of Syntax**

Syntax on page 1953
Syntax (EX Series Switch and the QFX Series) on page 1953

**Syntax**

```
show multicast usage
  <brief | detail>
  <inet | inet6>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

show multicast usage
  <brief | detail>
  <inet | inet6>
  <instance instance-name>

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display usage information about the 10 most active Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) groups.

**Options**

**none**—Display multicast usage information for all supported address families for all routing instances.

**brief | detail**—(Optional) Display the specified level of output.

**inet | inet6**—(Optional) Display usage information for IPv4 or IPv6 family addresses, respectively.

**instance instance-name**—(Optional) Display information about the most active DVMRP or PIM groups for a specific multicast instance.

**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 multicast usage on page 1954
show multicast usage brief on page 1954
show multicast usage instance on page 1954
show multicast usage detail on page 1955
Output Fields  
Table 107 on page 1954 describes the output fields for the `show multicast usage` command. Output fields are listed in the approximate order in which they appear.

Table 107: show multicast usage Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance. (Displayed when multicast is configured within a routing instance.)</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
</tr>
<tr>
<td>Sources</td>
<td>Number of sources.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the packets field displays unavailable.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of bytes that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the bytes field displays unavailable.</td>
</tr>
<tr>
<td>Prefix</td>
<td>IP address.</td>
</tr>
<tr>
<td>/len</td>
<td>Prefix length.</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of multicast groups.</td>
</tr>
<tr>
<td>Sensor ID</td>
<td>Sensor ID corresponding to multicast route.</td>
</tr>
</tbody>
</table>

Sample Output

**show multicast usage**

```
user@host> show multicast usage

Group           Sources Packets              Bytes
233.252.0.0       1       52847                4439148
233.252.0.1       2       13450                1125530

Prefix          /len Groups Packets              Bytes
10.255.14.144   /32  2      66254                5561304
10.255.70.15    /32  1      43                   3374...
```

**show multicast usage brief**

The output for the `show multicast usage brief` command is identical to that for the `show multicast usage` command. For sample output, see `show multicast usage on page 1954`.

**show multicast usage instance**

```
user@host> show multicast usage instance VPN-A
```
<table>
<thead>
<tr>
<th>Group</th>
<th>Sources</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>233.252.0.254</td>
<td>1</td>
<td>5538</td>
<td>509496</td>
</tr>
<tr>
<td>233.252.0.39</td>
<td>1</td>
<td>13</td>
<td>624</td>
</tr>
<tr>
<td>233.252.0.40</td>
<td>1</td>
<td>13</td>
<td>624</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prefix</th>
<th>/len</th>
<th>Groups</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.195.34</td>
<td>/32</td>
<td>1</td>
<td>5538</td>
<td>509496</td>
</tr>
<tr>
<td>10.255.14.30</td>
<td>/32</td>
<td>1</td>
<td>13</td>
<td>624</td>
</tr>
<tr>
<td>10.255.245.91</td>
<td>/32</td>
<td>1</td>
<td>13</td>
<td>624</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show multicast usage detail

```
user@host> show multicast usage detail

Group           Sources Packets              Bytes  
233.252.0.0     1       53159                4465356
233.252.0.1     2       13450                1122156
Source: 10.255.70.15 /32 Packets: 43 Bytes: 3374

Prefix          /len Groups Packets              Bytes  
10.255.14.144   /32  2      66566                5587512
Group: 233.252.0.0 Packets: 53159 Bytes: 4465356
Group: 233.252.0.1 Packets: 13407 Bytes: 1122156
10.255.70.15    /32  1      43                   3374
Group: 233.252.0.1 Packets: 43 Bytes: 3374
```
show pim bootstrap

List of Syntax  Syntax on page 1956
    Syntax (EX Series Switch and the QFX Series) on page 1956

Syntax  show pim bootstrap
       <instance instance-name>
       <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)  show pim bootstrap
       <instance instance-name>

Release Information  Command introduced before Junos OS Release 7.4.
                     Command introduced in Junos OS Release 9.0 for EX Series switches.
                     instance option introduced in Junos OS Release 10.0 for EX Series switches.
                     Command introduced in Junos OS Release 11.3 for the QFX Series.
                     Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  For sparse mode only, display information about Protocol Independent Multicast (PIM)
               bootstrap routers.

Options  none—Display PIM bootstrap router information for all routing instances.

           instance instance-name—(Optional) Display information about bootstrap routers for a
           specific PIM-enabled routing instance.

           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 pim bootstrap on page 1957
                       show pim bootstrap instance on page 1957

Output Fields  Table 108 on page 1956 describes the output fields for the show pim bootstrap command.
               Output fields are listed in the approximate order in which they appear.

Table 108: show pim bootstrap Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>BSR</td>
<td>Bootstrap router.</td>
</tr>
<tr>
<td>Pri</td>
<td>Priority of the routing device as elected to be the bootstrap router.</td>
</tr>
</tbody>
</table>
Table 108: show pim bootstrap Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local address</td>
<td>Local routing device address.</td>
</tr>
<tr>
<td>Pri</td>
<td>Local routing device address priority to be elected as the bootstrap router.</td>
</tr>
<tr>
<td>State</td>
<td>Local routing device election state: Candidate, Elected, or Ineligible.</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the local routing device declares the bootstrap router to be unreachable, in seconds.</td>
</tr>
</tbody>
</table>

Sample Output

show pim bootstrap

```
user@host> show pim bootstrap
Instance: PIM.master

<table>
<thead>
<tr>
<th>BSR</th>
<th>Pri</th>
<th>Local address</th>
<th>Pri State</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>10.255.71.46</td>
<td>0</td>
<td>InEligible</td>
</tr>
<tr>
<td>2001:db8:1:1:0:aff:785c</td>
<td>34</td>
<td>2001:db8:1:1:0:aff:7c12</td>
<td>0</td>
<td>InEligible</td>
</tr>
</tbody>
</table>
```

show pim bootstrap instance

```
user@host> show pim bootstrap instance VPN-A
Instance: PIM.VPN-A

<table>
<thead>
<tr>
<th>BSR</th>
<th>Pri</th>
<th>Local address</th>
<th>Pri State</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>192.168.196.105</td>
<td>0</td>
<td>InEligible</td>
</tr>
</tbody>
</table>
```
show pim interfaces

Syntax

```
show pim interfaces
<inet | inet6>
<instance (instance-name | all)>
<logical-system (all | logical-system-name)>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Support for the instance all option added in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about the interfaces on which Protocol Independent Multicast (PIM) is configured.

Options

none—Display interface information for all family addresses for the main instance.

inet | inet6—(Optional) Display interface information for IPv4 or IPv6 family addresses, respectively.

instance (instance-name | all)—(Optional) Display information about interfaces for a specific PIM-enabled routing instance or for all routing instances.

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 pim interfaces on page 1960
show pim interfaces (PIM using point-to-multipoint mode) on page 1960

Output Fields

Table 109 on page 1959 describes the output fields for the show pim interfaces command. Output fields are listed in the approximate order in which they appear.
Table 109: show pim interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Name</td>
<td>Interface name.</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface. The state also is displayed in the <code>show interfaces</code> command.</td>
</tr>
<tr>
<td>Mode</td>
<td>PIM mode running on the interface:</td>
</tr>
<tr>
<td></td>
<td>• B—In bidirectional mode, multicast groups are carried across the network over bidirectional shared trees. This type of tree minimizes PIM routing state, which is especially important in networks with numerous and dispersed senders and receivers.</td>
</tr>
<tr>
<td></td>
<td>• S—In sparse mode, routing devices must join and leave multicast groups explicitly. Upstream routing devices do not forward multicast traffic to this routing device unless this device has sent an explicit request (using a join message) to receive multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>• Dense—Unlike sparse mode, where data is forwarded only to routing devices sending an explicit request, dense mode implements a flood-and-prune mechanism, similar to DVMRP (the first multicast protocol used to support the multicast backbone). (Not supported on QFX Series.)</td>
</tr>
<tr>
<td></td>
<td>• Sparse-Dense—Sparse-dense mode allows the interface to operate on a per-group basis in either sparse or dense mode. A group specified as dense is not mapped to a rendezvous point (RP). Instead, data packets destined for that group are forwarded using PIM-Dense Mode (PIM-DM) rules. A group specified as sparse is mapped to an RP, and data packets are forwarded using PIM-Sparse Mode (PIM-SM) rules. When sparse-dense mode is configured, the output includes both S and D. When bidirectional-sparse mode is configured, the output includes S and B. When bidirectional-sparse-dense mode is configured, the output includes B, S, and D.</td>
</tr>
<tr>
<td>IP</td>
<td>Version number of the address family on the interface: 4 (IPv4) or 6 (IPv6).</td>
</tr>
<tr>
<td>V</td>
<td>PIM version running on the interface: 1 or 2.</td>
</tr>
<tr>
<td>State</td>
<td>State of PIM on the interface:</td>
</tr>
<tr>
<td></td>
<td>• Active—Bidirectional mode is enabled on the interface and on all PIM neighbors.</td>
</tr>
<tr>
<td></td>
<td>• DR—Designated router.</td>
</tr>
<tr>
<td></td>
<td>• NotCap—Bidirectional mode is not enabled on the interface. This can happen when bidirectional PIM is not configured locally, when one of the neighbors is not configured for bidirectional PIM, or when one of the neighbors has not implemented the bidirectional PIM protocol.</td>
</tr>
<tr>
<td></td>
<td>• NotDR—Not the designated router.</td>
</tr>
<tr>
<td></td>
<td>• P2P—Point to point.</td>
</tr>
<tr>
<td>NbrCnt</td>
<td>Number of neighbors that have been seen on the interface.</td>
</tr>
<tr>
<td>JoinCnt(sg)</td>
<td>Number of (s,g) join messages that have been seen on the interface.</td>
</tr>
<tr>
<td>JointCnt(*g)</td>
<td>Number of (*g) join messages that have been seen on the interface.</td>
</tr>
<tr>
<td>DR address</td>
<td>Address of the designated router.</td>
</tr>
</tbody>
</table>
### Sample Output

```bash
classic-router> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,  
S = Sparse, D = Dense, B = Bidirectional,  
DR = Designated Router, P2P = Point-to-point link,  
Active = Bidirectional is active, NotCap = Not Bidirectional Capable

<table>
<thead>
<tr>
<th>Name</th>
<th>Stat</th>
<th>Mode</th>
<th>IP</th>
<th>V</th>
<th>State</th>
<th>NbrCnt</th>
<th>JoinCnt(sg/*g)</th>
<th>DR address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/3/0.0</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2</td>
<td>NotDR,NotCap</td>
<td>1</td>
<td>0/0</td>
<td>40.0.0.3</td>
</tr>
<tr>
<td>ge-0/3/3.50</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2</td>
<td>DR,NotCap</td>
<td>1</td>
<td>9901/100</td>
<td>50.0.0.2</td>
</tr>
<tr>
<td>ge-0/3/3.51</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2</td>
<td>DR,NotCap</td>
<td>1</td>
<td>0/0</td>
<td>51.0.0.2</td>
</tr>
<tr>
<td>pe-1/2/0.32769</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2</td>
<td>P2P,NotCap</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
</tbody>
</table>

show pim interfaces (PIM using point-to-multipoint mode)

```
show pim join

List of Syntax  Syntax on page 1961
Syntax on page 1961
Syntax (EX Series Switch and the QFX Series) on page 1961

Syntax  
show pim join
<brief | detail | extensive | summary>
<bidirectional | dense | sparse>
<downstream-count>
<exact>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<range>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>

Syntax (EX Series Switch and the QFX Series)  
show pim join
<brief | detail | extensive | summary>
<dense | sparse>
<exact>
<inet | inet6>
<instance instance-name>
<range>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
summary option introduced in Junos OS Release 9.6.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Support for bidirectional PIM added in Junos OS Release 12.1.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Multiple new filter options introduced in Junos OS Release 13.2.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
downstream-count option introduced in Junos OS Release 16.1.
Support for PIM NSR support for VXLAN added in Junos OS Release 16.2
Support for RFC 5496 (via rpf-vector) added in Junos OS Release 17.3R1.

Description  Display information about Protocol Independent Multicast (PIM) groups for all PIM modes.
For bidirectional PIM, display information about PIM group ranges (*G-range) for each active bidirectional RP group range, in addition to each of the joined (*,G) routes.

Options  none—Display the standard information about PIM groups for all supported family addresses for all routing instances.
brief | detail | extensive | summary—(Optional) Display the specified level of output.

bidirectional | dense | sparse—(Optional) Display information about PIM bidirectional mode, dense mode, or sparse and source-specific multicast (SSM) mode entries.

downstream-count—(Optional) Display the downstream count instead of a list.

exact—(Optional) Display information about only the group that exactly matches the specified group address.

inet | inet6—(Optional) Display PIM group information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display information about groups for the specified PIM-enabled routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

range—(Optional) Address range of the group, specified as prefix/prefix-length.

rp ip-address/prefix | source ip-address/prefix—(Optional) Display information about the PIM entries with a specified rendezvous point (RP) address and prefix or with a specified source address and prefix. You can omit the prefix.

sg | star-g—(Optional) Display information about PIM (S,G) or (*G) entries.

Required Privilege Level

view

Related Documentation

- clear pim join on page 1816
- Example: Configuring Multicast-Only Fast Reroute in a PIM Domain
- Example: Configuring Bidirectional PIM
- Example: Configuring PIM State Limits

List of Sample Output

- show pim join summary on page 1966
- show pim join (PIM Sparse Mode) on page 1966
- show pim join (Bidirectional PIM) on page 1966
- show pim join inet6 on page 1967
- show pim join inet6 star-g on page 1968
- show pim join instance <instance-name> on page 1969
- show pim join instance <instance-name> downstream-count on page 1968
- show pim join instance <instance-name> downstream-count extensive on page 1969
- show pim join detail on page 1969
- show pim join extensive (PIM Resolve TLV for Multicast in Seamless MPLS) on page 1969
- show pim join extensive (PIM Sparse Mode) on page 1970
- show pim join extensive (Bidirectional PIM) on page 1971
**Output Fields**  
Table 110 on page 1963 describes the output fields for the `show pim join` 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>Instance</td>
<td>Name of the routing instance.</td>
<td>brief detail extensive summary none</td>
</tr>
<tr>
<td>Family</td>
<td>Name of the address family: <code>inet</code> (IPv4) or <code>inet6</code> (IPv6).</td>
<td>brief detail extensive summary none</td>
</tr>
<tr>
<td>Route type</td>
<td>Type of multicast route: <code>(S,G)</code> or <code>(*,G)</code>.</td>
<td>summary</td>
</tr>
<tr>
<td>Route count</td>
<td>Number of <code>(S,G)</code> routes and number of <code>(*,G)</code> routes.</td>
<td>summary</td>
</tr>
<tr>
<td>R</td>
<td>Rendezvous Point Tree.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>S</td>
<td>Sparse.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>W</td>
<td>Wildcard.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Bidirectional group prefix length</td>
<td>For bidirectional PIM, length of the IP prefix for RP group ranges.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Multicast source:</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <code>*</code> (wildcard value)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>ipv4-address</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>ipv6-address</code></td>
<td></td>
</tr>
<tr>
<td>RP</td>
<td>Rendezvous point for the PIM group.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>PIM flags:</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• <code>bidirectional</code>—Bidirectional mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>dense</code>—Dense mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>rptree</code>—Entry is on the rendezvous point tree.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>sparse</code>—Sparse mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>spt</code>—Entry is on the shortest-path tree for the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>wildcard</code>—Entry is on the shared tree.</td>
<td></td>
</tr>
</tbody>
</table>
Table 110: show pim join Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream interface</td>
<td>RPF interface toward the source address for the source-specific state (S,G) or toward the rendezvous point (RP) address for the non-source-specific state (*G). For bidirectional PIM, RP Link means that the interface is directly connected to a subnet that contains a phantom RP address. A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Upstream neighbor</td>
<td>Information about the upstream neighbor: Direct, Local, Unknown, or a specific IP address. For bidirectional PIM, Direct means that the interface is directly connected to a subnet that contains a phantom RP address. The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
<td>extensive</td>
</tr>
<tr>
<td>Upstream rpf-vector</td>
<td>Information about the upstream Reverse Path Forwarding (RPF) vector; appears in conjunction with the rpf-vector command.</td>
<td>extensive</td>
</tr>
<tr>
<td>Active upstream interface</td>
<td>When multicast-only fast reroute (MoFRR) is configured in a PIM domain, the upstream interface for the active path. A PIM router propagates join messages on two upstream RPF interfaces to receive multicast traffic on both links for the same join request. Preference is given to two paths that do not converge to the same immediate upstream router. PIM installs appropriate multicast routes with upstream neighbors as RPF next hops with two (primary and backup) interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td>Active upstream neighbor</td>
<td>On the MoFRR primary path, the IP address of the neighbor that is directly connected to the active upstream interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>MoFRR Backup upstream interface</td>
<td>The MoFRR upstream interface that is used when the primary path fails. When the primary path fails, the backup path is upgraded to primary, and traffic is forwarded accordingly. If there are alternate paths available, a new backup path is calculated and the appropriate multicast route is updated or installed.</td>
<td>extensive</td>
</tr>
<tr>
<td>MoFRR Backup upstream neighbor</td>
<td>IP address of the MoFRR upstream neighbor.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 110: show pim join 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>Upstream state</strong></td>
<td>Information about the upstream interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Join to RP</strong>—Sending a join to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Join to Source</strong>—Sending a join to the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local RP</strong>—Sending neither join messages nor prune messages toward the RP, because this routing device is the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local Source</strong>—Sending neither join messages nor prune messages toward the source, because the source is locally attached to this routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>No Prune to RP</strong>—Automatically sent to RP when SPT and RPT are on the same path.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Prune to RP</strong>—Sending a prune to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Prune to Source</strong>—Sending a prune to the source.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> RP group range entries have <strong>None</strong> in the Upstream state field because RP group ranges do not trigger actual PIM join messages between routing devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Downstream neighbors</strong></td>
<td>Information about downstream interfaces:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface</strong>—Interface name for the downstream neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pseudo PIM-SM interface appears for all IGMP-only interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pseudo multipoint LDP (Pseudo-MLDP) interface appears on ingress root nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface address</strong>—Address of the downstream neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—Information about the downstream neighbor: <strong>join</strong> or <strong>prune</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flags</strong>—PIM join flags: <strong>R</strong> (RPtree), <strong>S</strong> (Sparse), <strong>W</strong> (Wildcard), or <strong>zero</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Uptime</strong>—Time since the downstream interface joined the group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Time since last Join</strong>—Time since the last join message was received from the downstream interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Time since last Prune</strong>—Time since the last prune message was received from the downstream interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>rpf-vector</strong>—IP address of the RPF vector TLV.</td>
<td></td>
</tr>
<tr>
<td><strong>Number of downstream interfaces</strong></td>
<td>Total number of outgoing interfaces for each (S,G) entry.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Assert Timeout</strong></td>
<td>Length of time between assert cycles on the downstream interface. Not displayed if the assert timer is null.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Keepalive timeout</strong></td>
<td>Time remaining until the downstream join state is updated (in seconds). If the downstream join state is not updated before this keepalive timer reaches zero, the entry is deleted. If there is a directly connected host, <strong>Keepalive timeout</strong> is <strong>Infinity</strong>.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>Time since the creation of (S,G) or (<em>,G) state. The uptime is not refreshed every time a PIM join message is received for an existing (S,G) or (</em>,G) state.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
**Table 110: show pim join Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional accepting interfaces</td>
<td>Interfaces on the routing device that forward bidirectional PIM traffic.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>The reasons for forwarding bidirectional PIM traffic are that the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is the winner of the designated forwarder election (<strong>DF Winner</strong>), or the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface is the reverse path forwarding (<strong>RPF</strong>) interface toward the RP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(<strong>RPF</strong>).</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Output**

**show pim join summary**

```
user@host> show pim join summary
Instance: PIM.master Family: INET
Route type          Route count
  (s,g)              2
  (*,g)              1

Instance: PIM.master Family: INET6
```

**show pim join (PIM Sparse Mode)**

```
user@host> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.1
  Source: *
  RP: 10.255.14.144
  Flags: sparse,rptree,wildcard
  Upstream interface: Local

Group: 233.252.0.1
  Source: 10.255.14.144
  Flags: sparse,spt
  Upstream interface: Local

Group: 233.252.0.1
  Source: 10.255.70.15
  Flags: sparse,spt
  Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

**show pim join (Bidirectional PIM)**

```
user@host> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```
Group: 233.252.0.1
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0

Group: 233.252.0.2
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)

Group: 233.252.0.3
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0

Group: 233.252.0.4
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)

Instance: PIM.master
Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join inet6

user@host> show pim join inet6

Instance: PIM.master
Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 2001:db8::e000:101
  Source: *
  RP: ::46.0.0.13
  Flags: sparse,rptree,wildcard
  Upstream interface: Local

Group: 2001:db8::e000:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)

Group: 2001:db8::e800:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)

Group: 2001:db8::e800:101
  Source: ::1.1.1.2
  Flags: sparse
  Upstream interface: unknown (no neighbor)
show pim join inet6 star-g

user@host> show pim join inet6 star-g
Instance: PIM.master Family: INET6
  R = Rendezvous Point Tree, S = Sparse, W = Wildcard
Group: 2001:db8::e000:101
    Source: *
    RP: ::46.0.0.13
    Flags: sparse,rptree,wildcard
    Upstream interface: Local

show pim join instance <instance-name>

user@host> show pim join instance VPN-A
Instance: PIM.VPN-A Family: INET
  R = Rendezvous Point Tree, S = Sparse, W = Wildcard
Group: 233.252.0.2
    Source: *
    RP: 10.10.47.100
    Flags: sparse,rptree,wildcard
    Upstream interface: Local
Group: 233.252.0.2
    Source: 192.168.195.74
    Flags: sparse,spt
    Upstream interface: at-0/3/1.0
Group: 233.252.0.2
    Source: 192.168.195.169
    Flags: sparse
    Upstream interface: so-1/0/1.0

Instance: PIM.VPN-A Family: INET6
  R = Rendezvous Point Tree, S = Sparse, W = Wildcard
Group: 233.252.0.1
    Source: *
    RP: 10.11.11.6
    Flags: sparse,rptree,wildcard
    Upstream interface: mt-1/2/10.32813
    Number of downstream interfaces: 4
Group: 233.252.0.1
    Source: 10.1.1.1
    Flags: sparse,spt
    Upstream interface: ge-0/0/3.5
    Number of downstream interfaces: 5
show pim join instance <instance-name> downstream-count extensive

user@host> show pim join instance VPN-A downstream-count extensive

Instance: PIM.SML_VRF_4 Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.1
Source: *
RP: 10.11.11.6
Flags: sparse,rptree,wildcard
Upstream interface: mt-1/2/10.32813
Upstream neighbor: 10.2.2.7 (assert winner)
Upstream state: Join to RP
Uptime: 02:51:41
Number of downstream interfaces: 4
Number of downstream neighbors: 4

Group: 233.252.0.1
Source: 10.1.1.1
Flags: sparse,spt
Upstream interface: ge-0/0/3.5
Upstream neighbor: 10.1.1.17
Upstream state: Join to Source, Prune to RP
Keepalive timeout: 0
Uptime: 02:51:42
Number of downstream interfaces: 5
Number of downstream neighbors: 7

show pim join detail

user@host> show pim join detail

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 233.252.0.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local

Group: 233.252.0.1
Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join extensive (PIM Resolve TLV for Multicast in Seamless MPLS)

user@host> show pim join extensive
show pim join extensive (PIM Sparse Mode)

user@host> show pim join extensive

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Uptime: 00:03:49
Downstream neighbors:
  Interface: so-1/0/0.0
    10.111.10.2 State: Join Flags: SRW Timeout: 174
    Uptime: 00:03:49 Time since last Join: 00:01:49
    Interface: mt-1/1/0.32768
      10.10.47.100 State: Join Flags: SRW Timeout: Infinity
      Uptime: 00:03:49 Time since last Join: 00:01:49
Number of downstream interfaces: 2

Group: 233.252.0.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local Source, Local RP
Keepalive timeout: 344
Uptime: 00:03:49
Downstream neighbors:
  Interface: so-1/0/0.0
    10.111.10.2 State: Join Flags: S Timeout: 174
    Uptime: 00:03:49 Time since last Prune: 00:01:49
    Interface: mt-1/1/0.32768
      10.10.47.100 State: Join Flags: S Timeout: Infinity
      Uptime: 00:03:49 Time since last Prune: 00:01:49
Number of downstream interfaces: 2

Group: 233.252.0.1
Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0
Upstream neighbor: 10.111.10.2
Upstream state: Local RP, Join to Source
Keepalive timeout: 344
Uptime: 00:03:49
Downstream neighbors:
  Interface: Pseudo-GMP
  fe-0/0/0.0 fe-0/0/1.0 fe-0/0/3.0
  Interface: so-1/0/0.0 (pruned)
    10.111.10.2 State: Prune Flags: SR Timeout: 174
    Uptime: 00:03:49 Time since last Prune: 00:01:49
  Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: S Timeout: Infinity
    Uptime: 00:03:49 Time since last Prune: 00:01:49
Number of downstream interfaces: 3

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join extensive (Bidirectional PIM)

user@host> show pim join extensive

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0
  Upstream neighbor: 10.10.1.2
  Upstream state: None
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0 (RPF)
    Interface: lo0.0 (DF Winner)
  Number of downstream interfaces: 0

Group: 233.252.0.1
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0
  Upstream neighbor: 10.10.1.2
  Upstream state: None
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0 (RPF)
    Interface: lo0.0 (DF Winner)
  Downstream neighbors:
    Interface: lt-1/0/10.24
      10.0.24.4 State: Join RW Timeout: 185
show pim join extensive (Bidirectional PIM with a Directly Connected Phantom RP)

user@host> show pim join extensive

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.2
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)
Upstream neighbor: Direct
Upstream state: Local RP
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0 (RPF)
  Interface: lo0.0 (DF Winner)
  Interface: xe-4/1/0.0 (DF Winner)
Number of downstream interfaces: 0

show pim join instance <instance-name> extensive

user@host> show pim join instance VPN-A extensive

Instance: PIM.VPN-A Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.2
Source: *
RP: 10.10.47.100
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Uptime: 00:03:49
show pim join extensive (Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> **show pim join extensive**

<table>
<thead>
<tr>
<th>Instance</th>
<th>R</th>
<th>S</th>
<th>W</th>
<th>Group</th>
<th>Source</th>
<th>Flags</th>
<th>Upstream Interface</th>
<th>Upstream Neighbor</th>
<th>Upstream State</th>
<th>Keepalive timeout</th>
<th>Uptime</th>
<th>Group</th>
<th>Source</th>
<th>Flags</th>
<th>Upstream Interface</th>
<th>Upstream Neighbor</th>
<th>Upstream State</th>
<th>Keepalive timeout</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>S</td>
<td>W</td>
<td>233.252.0.3</td>
<td>192.168.219.11</td>
<td>sparse,spt</td>
<td>fe-1/3/1.0</td>
<td>Direct</td>
<td>Local Source</td>
<td></td>
<td>Downstream neighbors: Pseudo-MLDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show pim join extensive (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show pim join extensive

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 233.252.0.0
Source: *
RP: 10.1.1.1
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Uptime: 11:31:33
Downstream neighbors:
  Interface: fe-1/3/0.0
  192.168.209.9 State: Join Flags: SRW Timeout: Infinity
  Uptime: 11:31:33 Time since last Join: 11:31:32

Group: 233.252.0.1
Source: 192.168.219.11
Flags: sparse,spt
Upstream protocol: MLDP
Upstream interface: Pseudo MLDP
Upstream neighbor: MLDP LSP root <10.1.1.2>
Upstream state: Join to Source
Keepalive timeout:
Uptime: 11:31:32
Downstream neighbors:
  Interface: so-0/1/3.0
  192.168.92.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:30 Time since last Join: 11:31:30
Downstream neighbors:
  Interface: fe-1/3/0.0
  192.168.209.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 233.252.0.2
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <10.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
Downstream neighbors:
  Interface: so-0/1/3.0
  192.168.92.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:30 Time since last Join: 11:31:30
Downstream neighbors:
  Interface: lt-1/2/0.14
  10.1.4.4 State: Join Flags: S  Timeout: 177
  Uptime: 11:30:33 Time since last Join: 00:00:33
Downstream neighbors:
  Interface: fe-1/3/0.0
  192.168.209.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 233.252.0.3
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <10.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
Downstream neighbors:
  Interface: fe-1/3/0.0
  192.168.209.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 233.252.0.22
  Source: 10.2.7.7
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <10.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:30
Downstream neighbors:
  Interface: so-0/1/3.0
  192.168.92.9 State: Join Flags: S  Timeout: Infinity
  Uptime: 11:31:30 Time since last Join: 11:31:30
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 2001:db8::1:2
  Source: 2001:db8::1:2:7:7
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <10.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32

Downstream neighbors:
  Interface: fe-1/3/0.0
    2001:db8::21f:12ff:fea5:c4db State: Join Flags: S   Timeout: Infinity
    Uptime: 11:31:32 Time since last Join: 11:31:32
**show pim mdt**

**Syntax**

```
show pim mdt instance instance-name
  <brief | detail | extensive>
  data-mdt-joins
  data-mdt-limit
  inet
  inet6
  <incoming | outgoing>
  <logical-system (all | logical-system-name)>
  <range>
```

**Release Information**


**Description**

Display information about Protocol Independent Multicast (PIM) default multicast distribution tree (MDT) and the data MDTs in a Layer 3 VPN environment for a routing instance.

**Options**

- `instance instance-name`—Display information about data-MDTs for a specific PIM-enabled routing instance.
- `brief | detail | extensive`—(Optional) Display the specified level of output.
- `data-mdt-joins`—Show received PIM data-mdt-joins.
- `data-mdt-limits`—Show received PIM data-mdt-limits.
- `incoming | outgoing`—(Optional) Display incoming or outgoing multicast data tunnels, respectively.
- `inet | inet6`—Display IPv4 or IPv6 multicast data tunnels.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `range`—(Optional) Display information about an IP address with optional prefix length representing a particular multicast group.

**Required Privilege**

View

**List of Sample Output**

- `show pim mdt <variables> instance on page 1978`
- `show pim mdt instance detail on page 1979`
- `show pim mdt instance extensive on page 1979`
- `show pim mdt instance incoming on page 1980`
- `show pim mdt instance outgoing on page 1980`
- `show pim mdt instance (SSM Mode) on page 1980`
**Output Fields**  
Table 111 on page 1978 describes the output fields for the `show pim mdt` command. Output fields are listed in the approximate order in which they appear.

**Table 111: show pim mdt Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Tunnel direction</td>
<td>Direction the tunnel faces, from the router's perspective: <strong>Outgoing</strong> or <strong>Incoming</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Tunnel mode</td>
<td>Mode the tunnel is operating in: <strong>PIM-SSM</strong> or <strong>PIM-ASM</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Default group address</td>
<td>Default multicast group address using this tunnel.</td>
<td>All levels</td>
</tr>
<tr>
<td>Default source address</td>
<td>Default multicast source address using this tunnel.</td>
<td>All levels</td>
</tr>
<tr>
<td>Default tunnel interface</td>
<td>Default multicast tunnel interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Default tunnel source</td>
<td>Address used as the source address for outgoing PIM control messages.</td>
<td>All levels</td>
</tr>
<tr>
<td>C-Group</td>
<td>Customer-facing multicast group address using this tunnel. If you enable dynamic reuse of data MDT group addresses, more than one group address can use the same data MDT.</td>
<td>detail</td>
</tr>
<tr>
<td>C-Source</td>
<td>IP address of the multicast source in the customer's address space. If you enable dynamic reuse of data MDT group addresses, more than one source address can use the same data MDT.</td>
<td>detail</td>
</tr>
<tr>
<td>P-Group</td>
<td>Service provider-facing multicast group address using this tunnel.</td>
<td>detail</td>
</tr>
<tr>
<td>Data tunnel interface</td>
<td>Multicast data tunnel interface that set up the data-MDT tunnel.</td>
<td>detail</td>
</tr>
<tr>
<td>Last known forwarding rate</td>
<td>Last known rate, in kilobits per second, at which the tunnel was forwarding traffic.</td>
<td>detail</td>
</tr>
<tr>
<td>Configured threshold rate</td>
<td>Rate, in kilobits per second, above which a data-MDT tunnel is created and below which it is deleted.</td>
<td>detail</td>
</tr>
<tr>
<td>Tunnel uptime</td>
<td>Time that this data-MDT tunnel has existed. The format is <strong>hours:minutes:seconds</strong>.</td>
<td>detail</td>
</tr>
</tbody>
</table>

**Sample Output**

`show pim mdt <variables> instance`

Use this command to display MDT information for default MDT and data-MDT for IPv4 and/or IPv6 traffic. }
show pimdmt

Instance: PIM.VPN-A  Family: INET
Tunnel direction: Outgoing
Tunnel mode: PIM-SM
Default group address: 224.1.1.1
Default source address: 0.0.0.0
Default tunnel interface: mt-0/0/0.32768
Default tunnel source: 0.0.0.0

C-group address   C-source address   P-group address    Data tunnel interface
227.1.1.1         18.1.1.2           228.1.1.1          mt-0/0/0.32769

Instance: PIM.VPN-A
Tunnel direction: Incoming
Tunnel mode: PIM-SM
Default group address: 224.1.1.1
Default source address: 0.0.0.0
Default tunnel interface: mt-0/0/0.1081344
Default tunnel source: 0.0.0.0

Instance: PIM.VPN-A Family: INET6

show pimdmt instance detail

Instance: PIM.VPN-A
Tunnel direction: Outgoing
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.32768
Default tunnel source: 192.168.7.1
C-Group: 235.1.1.2
  C-Source: 192.168.195.74
  P-Group : 228.0.0.0
  Data tunnel interface : mt-1/1/0.32769
  Last known forwarding rate : 48 kbps (6 kbps)
  Configured threshold rate : 10 kbps
  Tunnel uptime : 00:00:34

Instance: PIM.VPN-A
Tunnel direction: Incoming
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.1081344

show pimdmt instance extensive

Instance: PIM.VPN-A
Tunnel direction: Outgoing
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.32768
Default tunnel source: 192.168.7.1
C-Group: 235.1.1.2
  C-Source: 192.168.195.74
  P-Group : 228.0.0.0
  Data tunnel interface : mt-1/1/0.32769
last known forwarding rate: 48 kbps (6 kbps)
configured threshold rate: 10 kbps
Tunnel uptime: 00:00:41

Instance: PIM.VPN-A
Tunnel direction: Incoming
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.1081344

show pim mdt instance incoming
user@host> show pim mdt instance VPN-A incoming
Instance: PIM.VPN-A
Tunnel direction: Incoming
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.1081344

show pim mdt instance outgoing
user@host> show pim mdt instance VPN-A outgoing
Instance: PIM.VPN-A
Tunnel direction: Outgoing
Default group address: 239.1.1.1
Default tunnel interface: mt-1/1/0.32768
Default tunnel source: 192.168.7.1

C-group address  C-source address  P-group address  Data tunnel interface
235.1.1.2       192.168.195.74     228.0.0.0       mt-1/1/0.32769

show pim mdt instance (SSM Mode)
user@host> show pim mdt instance vpn-a
Instance: PIM.vpn-a
Tunnel direction: Outgoing
Tunnel mode: PIM-SSM
Default group address: 232.1.1.1
Default source address: 10.255.14.216
Default tunnel interface: mt-1/3/0.32769
Default tunnel source: 192.168.7.1

Instance: PIM.vpn-a
Tunnel direction: Incoming
Tunnel mode: PIM-SSM
Default group address: 232.1.1.1
Default source address: 10.255.14.217
Default tunnel interface: mt-1/3/0.1081345

Instance: PIM.vpn-a
Tunnel direction: Incoming
Tunnel mode: PIM-SSM
Default group address: 232.1.1.1
Default source address: 10.255.14.218
Default tunnel interface: mt-1/3/0.1081345
show pim mdt data-mdt-joins

Syntax

```
show pim mdt data-mdt-joins
<logical-system (all | logical-system-name)> instance instance-name
```

Release Information

Command introduced in Junos OS Release 11.2.

Description

In a draft-rosen Layer 3 multicast virtual private network (MVPN) configured with service provider tunnels, display the advertisements of new multicast distribution tree (MDT) group addresses cached by the provider edge (PE) routers in the specified VPN routing and forwarding (VRF) instance that is configured to use the Protocol Independent Multicast (PIM) protocol.

Options

- **instance instance-name**—Display data MDT join packets cached by PE routers in a specific PIM instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**NOTE:** Draft-rosen multicast VPNs are not supported in a logical system environment even though the configuration statements can be configured under the logical-systems hierarchy.

Required Privilege Level

view

Related Documentation

- Understanding Data MDTs
- Example: Configuring Data MDTs and Provider Tunnels Operating in Source-Specific Multicast Mode
- Example: Configuring Data MDTs and Provider Tunnels Operating in Any-Source Multicast Mode

List of Sample Output

```
show pim mdt data-mdt-joins on page 1982
```

Output Fields

Table 112 on page 1982 describes the output fields for the `show pim mdt data-mdt-joins` command. Output fields are listed in the approximate order in which they appear.
Table 112: show pim mdt data-mdt-joins Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C-Group</strong></td>
<td>IPv4 group address in the address space of the customer’s VPN-specific PIM-enabled routing instance of the multicast traffic destination. This 32-bit value is carried in the C-group field of the MDT join TLV packet.</td>
</tr>
<tr>
<td><strong>C-Source</strong></td>
<td>IPv4 address in the address space of the customer’s VPN-specific PIM-enabled routing instance of the multicast traffic source. This 32-bit value is carried in the C-source field of the MDT join TLV packet.</td>
</tr>
<tr>
<td><strong>P-Group</strong></td>
<td>IPv4 group address in the service provider’s address space of the new data MDT that the PE router will use to encapsulate the VPN multicast traffic flow (C-Source, C-Group). This 32-bit value is carried in the P-group field of the MDT join TLV packet.</td>
</tr>
<tr>
<td><strong>P-Source</strong></td>
<td>IPv4 address of the PE router.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Timeout, in seconds, remaining for this cache entry. When the cache entry is created, this field is set to 180 seconds. After an entry times out, the PE router deletes the entry from its cache and prunes itself off the data MDT.</td>
</tr>
</tbody>
</table>

Sample Output

```
show pim mdt data-mdt-joins

user@host show pim mdt data-mdt-joins instance VPN-A

<table>
<thead>
<tr>
<th>C-Source</th>
<th>C-Group</th>
<th>P-Source</th>
<th>P-Group</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.2.15.9</td>
<td>225.1.1.2</td>
<td>20.0.0.5</td>
<td>239.10.10.0</td>
<td>172</td>
</tr>
<tr>
<td>20.2.15.9</td>
<td>225.1.1.3</td>
<td>20.0.0.5</td>
<td>239.10.10.1</td>
<td>172</td>
</tr>
</tbody>
</table>
```
show pim mdt data-mdt-limit

Syntax

show pim mdt data-mdt-limit instance instance-name
<logical-system (all | logical-system-name)>

Release Information

Command introduced in Junos OS Release 12.2.

Description

Display the maximum number configured and the currently active data multicast distribution trees (MDTs) for a specific VPN routing and forwarding (VRF) instance.

Options

instance instance-name—Display data MDT information for the specified VRF instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

NOTE: Draft-rosen multicast VPNs are not supported in a logical system environment even though the configuration statements can be configured under the logical-systems hierarchy.

Required Privilege

Level view

Related Documentation

- Understanding Data MDTs
- Example: Configuring Data MDTs and Provider Tunnels Operating in Source-Specific Multicast Mode
- Example: Configuring Data MDTs and Provider Tunnels Operating in Any-Source Multicast Mode

List of Sample Output

show pim mdt data-mdt-limit on page 1984

Output Fields

Table 113 on page 1983 describes the output fields for the show pim mdt data-mdt-limit command. Output fields are listed in the approximate order in which they appear.

Table 113: show pim mdt data-mdt-limit Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Data Tunnels</td>
<td>Maximum number of data MDTs created in this VRF instance. If the number is 0, no data MDTs are created for this VRF instance.</td>
</tr>
<tr>
<td>Active Data Tunnels</td>
<td>Active number of data MDTs in this VRF instance.</td>
</tr>
</tbody>
</table>
Sample Output

```
show pim mdt data-mdt-limit

user@host  show pim mdt data-mdt-limit instance VPN-A

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Data Tunnels</td>
<td>10</td>
</tr>
<tr>
<td>Active Data Tunnels</td>
<td>2</td>
</tr>
</tbody>
</table>
```
show pim neighbors

List of Syntax  Syntax on page 1985
Syntax (EX Series Switch and the QFX Series) on page 1985

Syntax  
show pim neighbors
  <brief | detail>
  <inet | inet6>
  <instance (instance-name | all)>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)  
show pim neighbors
  <brief | detail>
  <inet | inet6>
  <instance (instance-name | all)>

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Support for the instance all option added in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Support for RFC 5496 (via rpf-vector) added in Junos OS Release 17.3R1.

Description  
Display information about Protocol Independent Multicast (PIM) neighbors.

Options  
none—(Same as brief) Display standard information about PIM neighbors for all supported family addresses for the main instance.
brief | detail—(Optional) Display the specified level of output.
inet | inet6—(Optional) Display information about PIM neighbors for IPv4 or IPv6 family addresses, respectively.
instance (instance-name | all)—(Optional) Display information about neighbors for the specified PIM-enabled routing instance or for all routing instances.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege  
view

List of Sample Output  
show pim neighbors on page 1987
show pim neighbors instance on page 1987
show pim neighbors detail on page 1988
**Table 114: show pim neighbors Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor addr</td>
<td>Address of the neighboring PIM routing device.</td>
<td>All levels</td>
</tr>
<tr>
<td>IP</td>
<td>IP version: 4 or 6.</td>
<td>All levels</td>
</tr>
<tr>
<td>V</td>
<td>PIM version running on the neighbor: 1 or 2.</td>
<td>All levels</td>
</tr>
<tr>
<td>Mode</td>
<td>PIM mode of the neighbor: Sparse, Dense, SparseDense, or Unknown. When the neighbor is running PIM version 2, this mode is always Unknown.</td>
<td>All levels</td>
</tr>
<tr>
<td>Option</td>
<td>Can be one or more of the following:</td>
<td>brief none</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time the neighbor has been operational since the PIM process was last initialized.</td>
<td>All levels</td>
</tr>
<tr>
<td>Address</td>
<td>Address of the neighboring PIM routing device.</td>
<td>detail</td>
</tr>
<tr>
<td>BFD</td>
<td>Status and operational state of the Bidirectional Forwarding Detection (BFD) protocol on the interface: Enabled, Operational state is up, or Disabled.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Holdtime</td>
<td>Time for which the neighbor is available, in seconds. The range of values is 0 through 65,535.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Default Holdtime</td>
<td>Default holdtime and the time remaining if the holdtime option is not in the received hello message.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option DR Priority</td>
<td>Designated router election priority. The range of values is 0 through 255.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 114: show pim neighbors Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Option Join Attribute</td>
<td>Appears in conjunction with the rpf-vector command. The Join attribute is included in the PIM join messages of PIM routers that can receive type 1 Encoded-Source Address.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Generation ID</td>
<td>9-digit or 10-digit number used to tag hello messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Bi-Directional PIM supported</td>
<td>Neighbor can process bidirectional PIM messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option LAN Prune Delay</td>
<td>Time to wait before the neighbor receives prune messages, in the format delay nnn ms override mnn ms.</td>
<td>detail</td>
</tr>
<tr>
<td>Join Suppression supported</td>
<td>Neighbor is capable of join suppression.</td>
<td>detail</td>
</tr>
<tr>
<td>Rx Join</td>
<td>Information about joins received from the neighbor.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Group—Group addresses in the join message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Source—Address of the source in the join message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeout—Time for which the join is valid.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show pim neighbors

user@host> show pim neighbors

Instance: PIM.master
B = Bidirectional Capable, G = Generation Identifier, 
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay, 
P = Hello Option DR Priority, T = Tracking bit 
A = Hello Option Join Attribute

Instance: PIM.master
Interface | IP V Mode | Option       | Uptime | Neighbor addr
----------|-----------|--------------|--------|----------------
          | 4         | 2            |        | 19:01:24 20.0.0.13
          | 4         | 2            |        | 19:01:24 20.0.0.149

show pim neighbors instance

user@host> show pim neighbors instance VPN-A

Instance: PIM.VPN-A
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking bit

Interface | IP V Mode | Option | Uptime | Neighbor addr
----------|-----------|--------|--------|----------------
          | 4         | 2      |        | 00:07:54 10.111.30.2
show pim neighbors detail

user@host> show pim neighbors detail

Instance: PIM.master
Interface: ae1.0
Address: 20.0.0.149, IPv4, PIM v2, sg Join Count: 0, tsg Join Count: 332
BFD: Disabled
  Hello Option Holdtime: 105 seconds 86 remaining
  Hello Option DR Priority: 1
  Hello Option Generation ID: 853386212
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
  Join Suppression supported
  Hello Option Join Attribute supported
Address: 20.0.0.150, IPv4, PIM v2, Mode: SparseDense, sg Join Count: 0, tsg Join Count: 0
  Hello Option Holdtime: 65535 seconds
  Hello Option DR Priority: 1
  Hello Option Generation ID: 358917871
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
  Join Suppression supported
  Hello Option Join Attribute supported
Interface: lo0.0
Address: 10.255.179.246, IPv4, PIM v2, Mode: SparseDense, sg Join Count: 0, tsg Join Count: 0
  Hello Option Holdtime: 65535 seconds
  Hello Option DR Priority: 1
  Hello Option Generation ID: 1997462267
  Hello Option Bi-Directional PIM supported
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
  Join Suppression supported

show pim neighbors detail (With BFD)

user@host> show pim neighbors detail

Instance: PIM.master
Interface: fe-1/0/0.0
Address: 192.168.11.1, IPv4, PIM v2, Mode: Sparse
  Hello Option Holdtime: 65535 seconds
  Hello Option DR Priority: 1
  Hello Option Generation ID: 836607909
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Address: 192.168.11.2, IPv4, PIM v2
  BFD: Enabled, Operational state is up
  Hello Default Holdtime: 105 seconds 104 remaining
  Hello Option DR Priority: 1
  Hello Option Generation ID: 1907549685
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
<table>
<thead>
<tr>
<th>Interface: fe-1/0/1.0</th>
<th>Address: 192.168.12.1, IPv4, PIM v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD: Disabled</td>
<td></td>
</tr>
<tr>
<td>Hello Default Holdtime: 105 seconds 80 remaining</td>
<td></td>
</tr>
<tr>
<td>Hello Option DR Priority: 1</td>
<td></td>
</tr>
<tr>
<td>Hello Option Generation ID: 1971554705</td>
<td></td>
</tr>
<tr>
<td>Hello Option LAN Prune Delay: delay 500 ms override 2000 ms</td>
<td></td>
</tr>
</tbody>
</table>
show pim rps

**List of Syntax**

Syntax on page 1990
Syntax (EX Series Switch and the QFX Series) on page 1990

**Syntax**

```
show pim rps
<brief | detail | extensive>
<group-address>
/inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show pim rps
<brief | detail | extensive>
<group-address>
/inet | inet6>
<instance instance-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display information about Protocol Independent Multicast (PIM) rendezvous points (RPs).

**Options**

none—Display standard information about PIM RPs for all groups and family addresses for all routing instances.

brief | detail | extensive—(Optional) Display the specified level of output.

group-address—(Optional) Display the RPs for a particular group. If you specify a group address, the output lists the routing device that is the RP for that group.

/inet | inet6—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display information about RPs for a specific PIM-enabled routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

view
### Related Documentation

- *Example: Configuring Bidirectional PIM*

### List of Sample Output

- `show pim rps` on page 1993
- `show pim rps brief` on page 1994
- `show pim rps <group-address>` on page 1994
- `show pim rps <group-address>` on page 1994
- `show pim rps <group-address>` (Bidirectional PIM) on page 1994
- `show pim rps <group-address>` (PIM Dense Mode) on page 1994
- `show pim rps <group-address>` (SSM Range Without asm-override-ssm Configured) on page 1994
- `show pim rps <group-address>` (SSM Range With asm-override-ssm Configured and a Sparse-Mode RP) on page 1995
- `show pim rps <group-address>` (SSM Range With asm-override-ssm Configured and a Bidirectional RP) on page 1995
- `show pim rps instance` on page 1995
- `show pim rpsextensive (PIM Sparse Mode)` on page 1995
- `show pim rpsextensive (Bidirectional PIM)` on page 1996
- `show pim rpsextensive (PIM Anycast RP In Use)` on page 1996

### Output Fields

Table 115 on page 1991 describes the output fields for the `show pim rps` command. Output fields are listed in the approximate order in which they appear.

**Table 115: show pim rps Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Family or Address family</td>
<td>Name of the address family: <em>inet</em> (IPv4) or <em>inet6</em> (IPv6).</td>
<td>All levels</td>
</tr>
<tr>
<td>RP address</td>
<td>Address of the rendezvous point.</td>
<td>All levels</td>
</tr>
<tr>
<td>Type</td>
<td>Type of RP:</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>• auto-rp—Address of the RP known through the Auto-RP protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• bootstrap—Address of the RP known through the bootstrap router protocol (BSR).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• embedded—Address of the RP known through an embedded RP (IPv6).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• static—Address of RP known through static configuration.</td>
<td></td>
</tr>
<tr>
<td>Holdtime</td>
<td>How long to keep the RP active, with time remaining, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the local routing device determines the RP to be unreachable, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups currently using this RP.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group prefixes</td>
<td>Addresses of groups that this RP can span.</td>
<td>brief none</td>
</tr>
</tbody>
</table>
Table 115: `show pim rps` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learned via</td>
<td>Address and method by which the RP was learned.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mode</td>
<td>The PIM mode of the RP: bidirectional or sparse.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>If a sparse and bidirectional RPs are configured with the same RP address, they</td>
<td></td>
</tr>
<tr>
<td></td>
<td>appear as separate entries in both formats.</td>
<td></td>
</tr>
<tr>
<td>Time Active</td>
<td>How long the RP has been active, in the format hh:mm:ss.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Device Index</td>
<td>Index value of the order in which Junos OS finds and initializes the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>For bidirectional RPs, the Device Index output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.</td>
<td></td>
</tr>
<tr>
<td>Subunit</td>
<td>Logical unit number of the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>For bidirectional RPs, the Subunit output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Either the encapsulation or the de-encapsulation logical interface, depending on whether this routing device is a designated router (DR) facing an RP router, or is the local RP, respectively.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>For bidirectional RPs, the Interface output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.</td>
<td></td>
</tr>
<tr>
<td>Group Ranges</td>
<td>Addresses of groups that this RP spans.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Active groups using RP</td>
<td>Number of groups currently using this RP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>total</td>
<td>Total number of active groups for this RP.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 115: show pim rps 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>Register State for</strong></td>
<td><strong>RP</strong></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>Current register state for each group:</td>
<td></td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>Multicast group address.</td>
<td></td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Multicast source address for which the PIM register is sent or received, depending on whether this router is a designated router facing an RP router, or is the local RP, respectively:</td>
<td></td>
</tr>
<tr>
<td><strong>First Hop</strong></td>
<td>PIM-designated routing device that sent the Register message (the source address in the IP header).</td>
<td></td>
</tr>
<tr>
<td><strong>RP Address</strong></td>
<td>RP to which the Register message was sent (the destination address in the IP header).</td>
<td></td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>On the designated router:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Send</strong>—Sending Register messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Probe</strong>—Sent a null register. If a Register-Stop message does not arrive in 5 seconds, the designated router resumes sending Register messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suppress</strong>—Received a Register-Stop message. The designated router is waiting for the timer to resume before changing to <strong>Probe</strong> state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the RP:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Receive</strong>—Receiving Register messages.</td>
<td></td>
</tr>
<tr>
<td><strong>Anycast-PIM rpset</strong></td>
<td>If anycast RP is configured, the addresses of the RPs in the set.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Anycast-PIM local address used</strong></td>
<td>If anycast RP is configured, the local address used by the RP.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Anycast-PIM Register State</strong></td>
<td>If anycast RP is configured, the current register state for each group:</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>Multicast group address.</td>
<td></td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Multicast source address for which the PIM register is sent or received, depending on whether this routing device is a designated router facing an RP router, or is the local RP, respectively.</td>
<td></td>
</tr>
<tr>
<td><strong>Origin</strong></td>
<td>How the information was obtained:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>DIRECT</strong>—From a local attachment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MSDP</strong>—From the Multicast Source Discovery Protocol (MSDP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>DR</strong>—From the designated router</td>
<td></td>
</tr>
<tr>
<td><strong>RP selected</strong></td>
<td>For sparse mode and bidirectional mode, the identity of the RP for the specified group address.</td>
<td>group-address</td>
</tr>
</tbody>
</table>

Sample Output

```
user@host> show pim rps
Instance: PIM.master
Address-family INET
```
show pim rps brief

The output for the show pim rps brief command is identical to that for the show pim rps command. For sample output, see show pim rps on page 1993.

show pim rps <group-address>

user@host> show pim rps 233.252.0.0
Instance: PIM.master
Instance: PIM.master
RP selected: 10.100.100.100

show pim rps <group-address>

user@host> show pim rps 233.252.0.0
Instance: PIM.master
Instance: PIM.master
RP selected: 10.100.100.100

show pim rps <group-address> (Bidirectional PIM)

user@host> show pim rps 233.252.0.1
Instance: PIM.master

233.252.0.0/16
    10.4.12.75 (Bidirectional)

RP selected: 10.4.12.75

show pim rps <group-address> (PIM Dense Mode)

user@host> show pim rps 233.252.0.1
Instance: PIM.master

Dense Mode active for group 233.252.0.1

show pim rps <group-address> (SSM Range Without asm-override-ssm Configured)

user@host> show pim rps 233.252.0.1
Instance: PIM.master

Source-specific Mode (SSM) active for group 233.252.0.1
show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Sparse-Mode RP)

user@host> show pim rps 233.252.0.1

Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 233.252.0.1

233.252.0.0/16 10.4.12.75

RP selected: 10.4.12.75

show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Bidirectional RP)

user@host> show pim rps 233.252.0.1

Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 233.252.0.1

233.252.0.0/16 10.4.12.75 (Bidirectional)

RP selected: (null)

show pim rps instance

user@host> show pim rps instance VPN-A

Instance: PIM.VPN-A

Address family INET

<table>
<thead>
<tr>
<th>RP address</th>
<th>Type</th>
<th>Holdtime</th>
<th>Timeout</th>
<th>Groups</th>
<th>Group prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.47.100</td>
<td>static</td>
<td>0</td>
<td>None</td>
<td>1</td>
<td>233.252.0.0/4</td>
</tr>
</tbody>
</table>

Address family INET6

show pim rps extensive (PIM Sparse Mode)

user@host> show pim rps extensive

Instance: PIM.master

Family: INET

RP: 10.255.245.91

Learned via: static configuration

Time Active: 00:05:48

Holdtime: 45 with 36 remaining

Device Index: 122

Subunit: 32768

Interface: pd-6/0/0.32768

Group Ranges:

233.252.0.0/4, 36s remaining

Active groups using RP:

233.252.0.1

total 1 groups active

Chapter 19: IP Multicast Operational Commands
show pim rpsextensive (Bidirectional PIM)

```
user@host> show pim rpsextensive

Instance: PIM.master
Address family INET

RP: 10.10.1.3
Learned via: static configuration
Mode: Bidirectional
Time Active: 01:58:07
Holdtime: 150
Group Ranges:
    233.252.0.0/24
    233.252.0.1/24

RP: 10.10.13.2
Learned via: static configuration
Mode: Bidirectional
Time Active: 01:58:07
Holdtime: 150
Group Ranges:
    233.252.0.3/24
    233.252.0.4/24
```

show pim rpsextensive (PIM Anycast RP in Use)

```
user@host> show pim rpsextensive

Instance: PIM.master

Family: INET
RP: 10.10.10.2
Learned via: static configuration
Time Active: 00:54:52
Holdtime: 0
Device Index: 130
Subunit: 32769
Interface: pimd.32769
Group Ranges:
    233.252.0.0/4
Active groups using RP:
    233.252.0.10

    total 1 groups active

Anycast-PIM rpset:
    10.100.111.34
    10.100.111.17
    10.100.111.55

Anycast-PIM local address used: 10.100.111.1
Anycast-PIM Register State:
```
### Address family INET6

**Anycast-PIM rpset:**
- ab::1
- ab::2

**Anycast-PIM local address used:** cd::1

**Anycast-PIM Register State:**

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>::224.1.1.1</td>
<td>::10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>::224.1.1.2</td>
<td>::10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>::224.20.20.1</td>
<td>::10.10.71.1</td>
<td>DR</td>
</tr>
</tbody>
</table>
show pim snooping interfaces

Syntax

show pim snooping interfaces
  <brief | detail>
  <instance instance-name>
  <interface interface-name>
  <logical-system logical-system-name>
  <vlan-id vlan-identifier>

Release Information

Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

Description

Display information about PIM snooping interfaces.

Options

none—Display detailed information.
b brief | detail—(Optional) Display the specified level of output.
instance <instance-name>—(Optional) Display PIM snooping interface information for the specified routing instance.
interface <interface-name>—(Optional) Display PIM snooping information for the specified interface only.
logical-system logical-system-name—(Optional) Display information about a particular logical system, or type ’all’.
vlan-id <vlan-identifier>—(Optional) Display PIM snooping interface information for the specified VLAN.

Required Privilege

Level view

Related Documentation

• PIM Snooping for VPLS

List of Sample Output

show pim snooping interfaces on page 1999
show pim snooping interfaces instance vpls1 on page 1999
show pim snooping interfaces interface <interface-name> on page 2000
show pim snooping interfaces vlan-id <vlan-identifier> on page 2000

Output Fields

Table 116 on page 1999 lists the output fields for the show pim snooping interface command. Output fields are listed in the approximate order in which they appear.
Table 116: show pim snooping interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Routing instance for PIM snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Learning-Domain</td>
<td>Learning domain for snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Name</td>
<td>Router interfaces that are part of this learning domain.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: Up, or Down.</td>
<td>All levels</td>
</tr>
<tr>
<td>IP-Version</td>
<td>Version of IP used: 4 for IPv4, or 6 for IPv6.</td>
<td>All levels</td>
</tr>
<tr>
<td>NbrCnt</td>
<td>Number of neighboring routers connected through the specified interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>DR address</td>
<td>IP address of the designated router.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show pim snooping interfaces

user@host> show pim snooping interfaces
Instance: vpls1
Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
Name State IP-Version NbrCnt
ge-1/3/1.20 Up 4 1
ge-1/3/3.20 Up 4 1
ge-1/3/5.20 Up 4 1
ge-1/3/7.20 Up 4 1
DR address: 192.0.2.6
DR flooding is ON

show pim snooping interfaces instance vpls1

user@host> show pim snooping interfaces instance vpls1
Instance: vpls1

Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
Name State IP-Version NbrCnt
ge-1/3/1.20 Up 4 1
ge-1/3/2.20 Up 4 1
ge-1/3/3.20 Up 4 1
ge-1/3/5.20 Up 4 1
ge-1/3/7.20 Up 4 1
DR address: 192.0.2.6
DR flooding is ON

show pim snooping interfaces interface <interface-name>

user@host> show pim snooping interfaces interface ge-1/3/1.10
Instance: vpls1
Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON

Learning-Domain: vlan-id 20
DR address: 192.0.2.6
DR flooding is ON

show pim snooping interfaces vlan-id <vlan-id>

user@host> show pim snooping interfaces vlan-id 10
Instance: vpls1
Learning-Domain: vlan-id 10
Name State IP-Version NbrCnt
ge-1/3/1.10 Up 4 1
ge-1/3/3.10 Up 4 1
ge-1/3/5.10 Up 4 1
ge-1/3/7.10 Up 4 1
DR address: 192.0.2.5
DR flooding is ON
**show pim snooping join**

**Syntax**
```
show pim snooping join
  <brief | detail | extensive>
  <instance instance-name>
  <logical-system logical-system-name>
  <vlan-id vlan-id>
```

**Release Information**
- Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

**Description**
Display information about Protocol Independent Multicast (PIM) snooping joins.

**Options**
- `none`—Display detailed information.
- `brief | detail | extensive`—(Optional) Display the specified level of output.
- `instance instance-name`—(Optional) Display PIM snooping join information for the specified routing instance.
- `logical-system logical-system-name`—(Optional) Display information about a particular logical system, or type 'all'.
- `vlan-id vlan-identifier`—(Optional) Display PIM snooping join information for the specified VLAN.

**Required Privilege**
- `view`

**Related Documentation**
- *PIM Snooping for VPLS*

**List of Sample Output**
- show pim snooping join on page 2003
- show pim snooping join extensive on page 2003
- show pim snooping join instance on page 2003
- show pim snooping join vlan-id on page 2004

**Output Fields**
Table 117 on page 2001 lists the output fields for the `show pim snooping join` command. Output fields are listed in the approximate order in which they appear.

**Table 117: show pim snooping join Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Routing instance for PIM snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Learning-Domain</td>
<td>Learning domain for PIM snooping.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 117: show pim snooping join 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>Group</strong></td>
<td>Multicast group address.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Multicast source address:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• * (wildcard value)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;ipv4-address&gt;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;ipv6-address&gt;</code></td>
<td></td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>PIM flags:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• bidirectional—Bidirectional mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• dense—Dense mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rptree—Entry is on the rendezvous point tree.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sparse—Sparse mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• spt—Entry is on the shortest-path tree for the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• wildcard—Entry is on the shared tree.</td>
<td></td>
</tr>
<tr>
<td><strong>Upstream state</strong></td>
<td>Information about the upstream interface:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Join to RP—Sending a join to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Join to Source—Sending a join to the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Local RP—Sending neither join messages nor prune messages toward the RP, because this router is the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Local Source—Sending neither join messages nor prune messages toward the source, because the source is locally attached to this routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prune to RP—Sending a prune to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Prune to Source—Sending a prune to the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> RP group range entries have None in the Upstream state field because RP group ranges do not trigger actual PIM join messages between routers.</td>
<td></td>
</tr>
<tr>
<td><strong>Upstream neighbor</strong></td>
<td>Information about the upstream neighbor: Direct, Local, Unknown, or a specific IP address.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>For bidirectional PIM, Direct means that the interface is directly connected to a subnet that contains a phantom RP address.</td>
<td></td>
</tr>
<tr>
<td><strong>Upstream port</strong></td>
<td>RPF interface toward the source address for the source-specific state (S,G) or toward the rendezvous point (RP) address for the non-source-specific state (*G).</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>For bidirectional PIM, RP Link means that the interface is directly connected to a subnet that contains a phantom RP address.</td>
<td></td>
</tr>
<tr>
<td><strong>Downstream port</strong></td>
<td>Information about downstream interfaces.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Downstream neighbors</strong></td>
<td>Address of the downstream neighbor.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Time remaining until the downstream join state is updated (in seconds).</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Sample Output

show pim snooping join

```
user@host> show pim snooping join

Instance: vpls1

Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10

Learning-Domain: vlan-id 20
Group: 198.51.100.3
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 203.0.113.4, port: ge-1/3/5.20
```

show pim snooping join extensive

```
user@host> show pim snooping join extensive

Instance: vpls1

Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10
Downstream port: ge-1/3/1.10
Downstream neighbors:
192.0.2.2 State: Join Flags: SRW Timeout: 166

Learning-Domain: vlan-id 20
Group: 198.51.100.3
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 203.0.113.4, port: ge-1/3/5.20
Downstream port: ge-1/3/3.20
Downstream neighbors:
203.0.113.3 State: Join Flags: SRW Timeout: 168
```

show pim snooping join instance

```
user@host> show pim snooping join instance vpls1

Instance: vpls1

Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
```
show pim snooping join vlan-id

user@host> show pim snooping join vlan-id 10

Instance: vpls1
Learning-Domain: vlan-id 10
Group: 198.51.100.2
Source: *
Flags: sparse,rptree,wildcard
Upstream state: None
Upstream neighbor: 192.0.2.4, port: ge-1/3/5.10
**show pim snooping neighbors**

**Syntax**
```
show pim snooping neighbors
  <brief | detail>
  <instance instance-name>
  <interface interface-name>
  <logical-system logical-system-name>
  <vlan-id vlan-identifier>
```

**Release Information**
Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

**Description**
Display information about Protocol Independent Multicast (PIM) snooping neighbors.

**Options**
- **none**—Display detailed information.
- **brief | detail**—(Optional) Display the specified level of output.
- **instance instance-name**—(Optional) Display PIM snooping neighbor information for the specified routing instance.
- **interface interface-name**—(Optional) Display information for the specified PIM snooping neighbor interface.
- **logical-system logical-system-name**—(Optional) Display information about a particular logical system, or type 'all'.
- **vlan-id vlan-identifier**—(Optional) Display PIM snooping neighbor information for the specified VLAN.

**Required Privilege Level**
view

**Related Documentation**
- Configuring Interface Priority for PIM Designated Router Selection
- Modifying the PIM Hello Interval
- PIM Snooping for VPLS
- show pim neighbors on page 1985

**List of Sample Output**
- show pim snooping neighbors on page 2006
- show pim snooping neighbors detail on page 2007
- show pim snooping neighbors instance on page 2008
- show pim snooping neighbors interface on page 2009
- show pim snooping neighbors vlan-id on page 2009
Output Fields  Table 118 on page 2006 lists the output fields for the show pim snooping 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>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Routing instance for PIM snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Learning-Domain</td>
<td>Learning domain for PIM snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Router interface for which PIM snooping neighbor details are displayed.</td>
<td>All levels</td>
</tr>
<tr>
<td>Option</td>
<td>PIM snooping options available on the specified interface:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• H = Hello Option Holdtime</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• P = Hello Option DR Priority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L = Hello Option LAN Prune Delay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• G = Generation Identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T = Tracking Bit</td>
<td></td>
</tr>
<tr>
<td>Uptime</td>
<td>Time the neighbor has been operational since the PIM process was last initialized, in the format dd:hh:mm:ss ago for less than a week and nwnd:hh:mm:ss ago for more than a week.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor addr</td>
<td>IP address of the PIM snooping neighbor connected through the specified interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the specified router interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hello Option Holdtime</td>
<td>Time for which the neighbor is available, in seconds. The range of values is 0 through 65,535.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option DR Priority</td>
<td>Designated router election priority. The range of values is 0 through 4294967295.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: By default, every PIM interface has an equal probability (priority 1) of being selected as the DR.</td>
<td></td>
</tr>
<tr>
<td>Hello Option Generation ID</td>
<td>9-digit or 10-digit number used to tag hello messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option LAN Prune Delay</td>
<td>Time to wait before the neighbor receives prune messages, in the format delay nnn ms override nnnn ms.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show pim snooping neighbors

user@host> show pim snooping neighbors

B = Bidirectional Capable, G = Generation Identifier, H = Hello Option Holdtime, L = Hello Option LAN Prune Delay, P = Hello Option DR Priority, T = Tracking Bit
show pim snooping neighbors detail

user@host> show pim snooping neighbors detail

Instance: vpls1
Learning-Domain: vlan-id 10

Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:43:33 192.0.2.2
ge-1/3/3.10 HPLGT 00:43:33 192.0.2.3
ge-1/3/5.10 HPLGT 00:43:33 192.0.2.4
ge-1/3/7.10 HPLGT 00:43:33 192.0.2.5

Learning-Domain: vlan-id 20

Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:43:33 192.0.2.12
ge-1/3/3.20 HPLGT 00:43:33 192.0.2.13
ge-1/3/5.20 HPLGT 00:43:33 192.0.2.14
ge-1/3/7.20 HPLGT 00:43:33 192.0.2.15
show pim snooping neighbors instance

user@host> show pim snooping neighbors instance vpls1

B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: vpls1
Learning-Domain: vlan-id 10

Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:46:03 192.0.2.2
ge-1/3/3.10 HPLGT 00:46:03 192.0.2.2
ge-1/3/5.10 HPLGT 00:46:03 192.0.2.2
ge-1/3/7.10 HPLGT 00:46:03 192.0.2.2

Learning-Domain: vlan-id 20

Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:46:03 192.0.2.12
ge-1/3/3.20 HPLGT 00:46:03 192.0.2.13
show pim snooping neighbors interface

user@host> show pim snooping neighbors interface ge-1/3/1.20

B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

Interface Option Uptime Neighbor addr
ge-1/3/1.20 HPLGT 00:48:04 192.0.2.12

show pim snooping neighbors vlan-id

user@host> show pim snooping neighbors vlan-id 10

B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority, T = Tracking Bit

Instance: vpls1
Learning-Domain: vlan-id 10

Interface Option Uptime Neighbor addr
ge-1/3/1.10 HPLGT 00:49:12 192.0.2.2
ge-1/3/3.10 HPLGT 00:49:12 192.0.2.3
ge-1/3/5.10 HPLGT 00:49:12 192.0.2.4
ge-1/3/7.10 HPLGT 00:49:12 192.0.2.5
**show pim snooping statistics**

**Syntax**
```
show pim snooping statistics
  <instance instance-name>
  <interface interface-name>
  <logical-system logical-system-name>
  <vlan-id vlan-id>
```

**Release Information**
Command introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.

**Description**
Display Protocol Independent Multicast (PIM) snooping statistics.

**Options**
- `none`—Display PIM statistics.
- `instance instance-name`—(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM) snooping.
- `interface interface-name`—(Optional) Display statistics about the specified interface for PIM snooping.
- `logical-system logical-system-name`—(Optional) Display information about a particular logical system, or type 'all'.
- `vlan-id vlan-identifier`—(Optional) Display PIM snooping statistics information for the specified VLAN.

**Required Privilege Level**
view

**Related Documentation**
- *PIM Snooping for VPLS*
- clear pim snooping statistics on page 1824

**List of Sample Output**
- show pim snooping statistics on page 2011
- show pim snooping statistics instance on page 2012
- show pim snooping statistics interface on page 2013
- show pim snooping statistics vlan-id on page 2013

**Output Fields**
Table 119 on page 2010 lists the output fields for the `show pim snooping statistics` 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>Instance</td>
<td>Routing instance for PIM snooping.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Table 119: `show pim snooping statistics` Output Fields
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learning-Domain</td>
<td>Learning domain for PIM snooping.</td>
<td>All levels</td>
</tr>
<tr>
<td>Tx J/P messages</td>
<td>Total number of transmitted join/prune packets.</td>
<td>All levels</td>
</tr>
<tr>
<td>RX J/P messages</td>
<td>Total number of received join/prune packets.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx J/P messages -- seen</td>
<td>Number of join/prune packets seen but not received on the upstream interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx J/P messages -- received</td>
<td>Number of join/prune packets received on the downstream interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Hello messages</td>
<td>Total number of received hello packets.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Version Unknown</td>
<td>Number of packets received with an unknown version number.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Neighbor Unknown</td>
<td>Number of packets received from an unknown neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Upstream Neighbor Unknown</td>
<td>Number of packets received with unknown upstream neighbor information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Bad Length</td>
<td>Number of packets received containing incorrect length information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx J/P Busy Drop</td>
<td>Number of join/prune packets dropped while the router is busy.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx J/P Group Aggregate 0</td>
<td>Number of join/prune packets received containing the aggregate group information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Malformed Packet</td>
<td>Number of malformed packets received.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx No PIM Interface</td>
<td>Number of packets received without the interface information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx No Upstream Neighbor</td>
<td>Number of packets received without upstream neighbor information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rx Unknown Hello Option</td>
<td>Number of hello packets received with unknown options.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

**Sample Output**

`show pim snooping statistics`

```
user@host> show pim snooping statistics
```
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 8
Rx J/P messages -- seen 0
Rx J/P messages -- received 8
Rx Hello messages 37
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0

Learning-Domain: vlan-id 20

Tx J/P messages 0
RX J/P messages 2
Rx J/P messages -- seen 0
Rx J/P messages -- received 2
Rx Hello messages 39
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
Rx Unknown Hello Option 0
Rx Malformed Packet 0

show pim snooping statistics instance

user@host> show pim snooping statistics instance vpls1

Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 9
Rx J/P messages -- seen 0
Rx J/P messages -- received 9
Rx Hello messages 45
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
show pim snooping statistics interface

user@host> show pim snooping statistics interface ge-1/3/1.20

Instance: vpls1
Learning-Domain: vlan-id 10
Learning-Domain: vlan-id 20

PIM Interface statistics for ge-1/3/1.20
Tx J/P messages 0
RX J/P messages 0
Rx J/P messages -- seen 0
Rx J/P messages -- received 0
Rx Hello messages 13
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0

show pim snooping statistics vlan-id

user@host> show pim snooping statistics vlan-id 10
Instance: vpls1
Learning-Domain: vlan-id 10

Tx J/P messages 0
RX J/P messages 11
Rx J/P messages -- seen 0
Rx J/P messages -- received 11
Rx Hello messages 64
Rx Version Unknown 0
Rx Neighbor Unknown 0
Rx Upstream Neighbor Unknown 0
Rx Bad Length 0
Rx J/P Busy Drop 0
Rx J/P Group Aggregate 0
Rx Malformed Packet 0
Rx No PIM Interface 0
Rx No Upstream Neighbor 0
Rx Bad Length 0
Rx Neighbor Unknown 0
**show pim source**

**List of Syntax**

Syntax on page 2015
Syntax (EX Series Switch and the QFX Series) on page 2015

**Syntax**

show pim source

- `<brief | detail>`
- `<inet | inet6>`
- `<instance instance-name>`
- `<logical-system (all | logical-system-name)>`
- `<source-prefix>`

**Syntax (EX Series Switch and the QFX Series)**

show pim source

- `<brief | detail>`
- `<inet | inet6>`
- `<instance instance-name>`
- `<source-prefix>`

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display information about the Protocol Independent Multicast (PIM) source reverse path forwarding (RPF) state.

**Options**

- `none`—Display standard information about the PIM RPF state for all supported family addresses for all routing instances.

- `brief | detail`—(Optional) Display the specified level of output.

- `inet | inet6`—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.

- `instance instance-name`—(Optional) Display information about the RPF state for a specific PIM-enabled routing instance.

- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

- `source-prefix`—(Optional) Display the state for source RPF states in the given range.

**Required Privilege Level**

view

**List of Sample Output**

- show pim source on page 2016
- show pim source brief on page 2016
- show pim source detail on page 2017
show pim source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2017

Output Fields  Table 120 on page 2016 describes the output fields for the `show pim source` command. Output fields are listed in the approximate order in which they appear.

Table 120: show pim source Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Source</td>
<td>Address of the source or reverse path.</td>
</tr>
<tr>
<td>Prefix/length</td>
<td>Prefix and prefix length for the route used to reach the RPF address.</td>
</tr>
<tr>
<td>Upstream Protocol</td>
<td>Protocol toward the source address.</td>
</tr>
<tr>
<td>Upstream interface</td>
<td>RPF interface toward the source address.</td>
</tr>
<tr>
<td></td>
<td>A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>Address of the RPF neighbor used to reach the source address.</td>
</tr>
<tr>
<td></td>
<td>The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
</tr>
</tbody>
</table>

Sample Output

show pim source

user@host> show pim source

Instance: PIM.master Family: INET

Source 10.255.14.44
Prefix 10.255.14.44/32
Upstream interface Local
Upstream neighbor Local

Source 10.255.70.15
Prefix 10.255.70.15/32
Upstream interface so-1/0/0.0
Upstream neighbor 10.111.10.2

Instance: PIM.master Family: INET6

show pim source brief

The output for the `show pim source brief` command is identical to that for the `show pim source` command. For sample output, see `show pim source` on page 2016.
show pim source detail

user@host> show pim source detail

Instance: PIM.master Family: INET

Source 10.255.14.144
  Prefix 10.255.14.144/32
  Upstream interface Local
  Upstream neighbor Local
  Active groups:233.252.0.0
    233.252.0.1
    233.252.0.1

Source 10.255.70.15
  Prefix 10.255.70.15/32
  Upstream interface so-1/0/0.0
  Upstream neighbor 10.111.10.2
  Active groups:233.252.0.1

Instance: PIM.master Family: INET6

show pim source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show pim source

Instance: PIM.master Family: INET

Source 10.1.1.1
  Prefix 10.1.1.1/32
  Upstream interface Local
  Upstream neighbor Local

Source 10.2.7.7
  Prefix 10.2.7.0/24
  Upstream protocol MLDP
  Upstream interface Pseudo MLDP
  Upstream neighbor MLDP LSP root <10.1.1.2>

Source 192.168.219.11
  Prefix 192.168.219.0/28
  Upstream protocol MLDP
  Upstream interface Pseudo MLDP
  Upstream neighbor via MLDP-inband
  Upstream interface fe-1/3/0.0
  Upstream neighbor 192.168.140.1
  Upstream neighbor MLDP LSP root <10.1.1.2>

Instance: PIM.master Family: INET6

Source 2001:db8::1:2:7:7
  Prefix 2001:db8::1:2:7:0/120
  Upstream protocol MLDP
  Upstream interface Pseudo MLDP
  Upstream neighbor via MLDP-inband
  Upstream interface fe-1/3/0.0
  Upstream neighbor 192.168.140.1
  Upstream neighbor MLDP LSP root <10.1.1.2>
**show pim statistics**

**List of Syntax**

Syntax (EX Series Switch and the QFX Series) on page 2018

Syntax

```
show pim statistics
<inet | inet6>  
<instance instance-name>
@interface interface-name>
<logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display Protocol Independent Multicast (PIM) statistics.

**Options**

`none`—Display PIM statistics.

`inet | inet6`—(Optional) Display IPv4 or IPv6 PIM statistics, respectively.

`instance instance-name`—(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM).

`interface interface-name`—(Optional) Display statistics about the specified interface.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

`view`

**Related Documentation**

- clear pim statistics on page 1826

**List of Sample Output**

show pim statistics on page 2025
show pim statistics inet interface <interface-name> on page 2027
show pim statistics inet6 interface <interface-name> on page 2027
show pim statistics instance <instance-name> on page 2028
Output Fields  

Table 121 on page 2019 describes the output fields for the `show pim statistics` command. Output fields are listed in the approximate order in which they appear.

*Table 121: show pim statistics Output Fields*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Instance       | Name of the routing instance. This field only appears if you specify an interface, for example:  
                    - `inet interface interface-name`  
                    - `inet6 interface interface-name`  
                    - `interface interface-name`  |
| Family         | Output is for IPv4 or IPv6 PIM statistics. INET indicates IPv4 statistics, and INET6 indicates IPv6 statistics. This field only appears if you specify an interface, for example:  
                    - `inet interface interface-name`  
                    - `inet6 interface interface-name`  
                    - `interface interface-name`  |
| PIM statistics | PIM statistics for all interfaces or for the specified interface.                  |
| PIM message type| Message type for which statistics are displayed.                                    |
| Received       | Number of received statistics.                                                     |
| Sent           | Number of messages sent of a certain type.                                         |
| Rx errors      | Number of received packets that contained errors.                                   |
| V2 Hello       | PIM version 2 hello packets.                                                       |
| V2 Register    | PIM version 2 register packets.                                                     |
| V2 Register Stop| PIM version 2 register stop packets.                                                |
| V2 Join Prune  | PIM version 2 join and prune packets.                                               |
| V2 Bootstrap   | PIM version 2 bootstrap packets.                                                    |
| V2 Assert      | PIM version 2 assert packets.                                                       |
| V2 Graft       | PIM version 2 graft packets.                                                        |
| V2 Graft Ack   | PIM version 2 graft acknowledgment packets.                                         |
| V2 Candidate RP| PIM version 2 candidate RP packets.                                                 |
Table 121: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 State Refresh</td>
<td>PIM version 2 control messages related to PIM dense mode (PIM-DM) state refresh.</td>
</tr>
<tr>
<td></td>
<td>State refresh is an extension to PIM-DM. It not supported in Junos OS.</td>
</tr>
<tr>
<td>V2 DF Election</td>
<td>PIM version 2 send and receive messages associated with bidirectional PIM designated forwarder election.</td>
</tr>
<tr>
<td>V1 Query</td>
<td>PIM version 1 query packets.</td>
</tr>
<tr>
<td>V1 Register</td>
<td>PIM version 1 register packets.</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>PIM version 1 register stop packets.</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>PIM version 1 join and prune packets.</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>PIM version 1 RP reachability packets.</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>PIM version 1 assert packets.</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>PIM version 1 graft packets.</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>PIM version 1 graft acknowledgment packets.</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>Auto-RP mapping packets.</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>Auto-RP packets with an unknown type.</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>Global Statistics</td>
<td>Summary of PIM statistics for all interfaces.</td>
</tr>
<tr>
<td>Hello dropped on neighbor policy</td>
<td>Number of hello packets dropped because of a configured neighbor policy.</td>
</tr>
<tr>
<td>Unknown type</td>
<td>Number of PIM control packets received with an unknown type.</td>
</tr>
<tr>
<td>V1 Unknown type</td>
<td>Number of PIM version 1 control packets received with an unknown type.</td>
</tr>
<tr>
<td>Unknown Version</td>
<td>Number of PIM control packets received with an unknown version. The version is not version 1 or version 2.</td>
</tr>
</tbody>
</table>
### Table 12: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor unknown</td>
<td>Number of PIM control packets received (excluding PIM hello) without first receiving the hello packet.</td>
</tr>
<tr>
<td>Bad Length</td>
<td>Number of PIM control packets received for which the packet size does not match the PIM length field in the packet.</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>Number of PIM control packets received for which the calculated checksum does not match the checksum field in the packet.</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>Number of PIM control packets received on an interface that does not have PIM configured.</td>
</tr>
<tr>
<td>Rx Bad Data</td>
<td>Number of PIM control packets received that contain data for TCP Bad register packets.</td>
</tr>
<tr>
<td>Rx Intf disabled</td>
<td>Number of PIM control packets received on an interface that has PIM disabled.</td>
</tr>
<tr>
<td>Rx V1 Require V2</td>
<td>Number of PIM version 1 control packets received on an interface configured for PIM version 2.</td>
</tr>
<tr>
<td>Rx V2 Require V1</td>
<td>Number of PIM version 2 control packets received on an interface configured for PIM version 1.</td>
</tr>
<tr>
<td>Rx Register not RP</td>
<td>Number of PIM register packets received when the routing device is not the RP for the group.</td>
</tr>
<tr>
<td>Rx Register no route</td>
<td>Number of PIM register packets received when the RP does not have a unicast route back to the source.</td>
</tr>
<tr>
<td>Rx Register no decap if</td>
<td>Number of PIM register packets received when the RP does not have a de-encapsulation interface.</td>
</tr>
<tr>
<td>Null Register Timeout</td>
<td>Number of NULL register timeout packets.</td>
</tr>
<tr>
<td>RP Filtered Source</td>
<td>Number of PIM packets received when the routing device has a source address filter configured for the RP.</td>
</tr>
<tr>
<td>Rx Unknown Reg Stop</td>
<td>Number of register stop messages received with an unknown type.</td>
</tr>
<tr>
<td>Rx Join/Prune no state</td>
<td>Number of join and prune messages received for which the routing device has no state.</td>
</tr>
<tr>
<td>Rx Join/Prune on upstream if</td>
<td>Number of join and prune messages received on the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Rx Join/Prune for invalid group</td>
<td>Number of join or prune messages received for invalid multicast group addresses.</td>
</tr>
</tbody>
</table>
### Table 12: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Join/Prune messages dropped</td>
<td>Number of join and prune messages received and dropped.</td>
</tr>
<tr>
<td>Rx sparse join for dense group</td>
<td>Number of PIM sparse mode join messages received for a group that is configured for dense mode.</td>
</tr>
<tr>
<td>Rx Graft/Graft Ack no state</td>
<td>Number of graft and graft acknowledgment messages received for which the router or switch has no state.</td>
</tr>
<tr>
<td>Rx Graft on upstream if</td>
<td>Number of graft messages received on the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Rx CRP not BSR</td>
<td>Number of BSR messages received in which the PIM message type is Candidate-RP-Advertisement, not Bootstrap.</td>
</tr>
<tr>
<td>Rx BSR when BSR</td>
<td>Number of BSR messages received in which the PIM message type is Bootstrap.</td>
</tr>
<tr>
<td>Rx BSR not RPF if</td>
<td>Number of BSR messages received on an interface that is not the RPF interface.</td>
</tr>
<tr>
<td>Rx unknown hello opt</td>
<td>Number of PIM hello packets received with options that Junos OS does not support.</td>
</tr>
<tr>
<td>Rx data no state</td>
<td>Number of PIM control packets received for which the routing device has no state for the data type.</td>
</tr>
<tr>
<td>Rx RP no state</td>
<td>Number of PIM control packets received for which the routing device has no state for the RP.</td>
</tr>
<tr>
<td>Rx aggregate</td>
<td>Number of PIM aggregate MDT packets received.</td>
</tr>
<tr>
<td>Rx malformed packet</td>
<td>Number of PIM control packets received with a malformed IP unicast or multicast address family.</td>
</tr>
<tr>
<td>No RP</td>
<td>Number of PIM control packets received with no RP address.</td>
</tr>
<tr>
<td>No register encap if</td>
<td>Number of PIM register packets received when the first-hop routing device does not have an encapsulation interface.</td>
</tr>
<tr>
<td>No route upstream</td>
<td>Number of PIM control packets received when the routing device does not have a unicast route to the the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Nexthop Unusable</td>
<td>Number of PIM control packets with an unusable nexthop. A path can be unusable if the route is hidden or the link is down.</td>
</tr>
<tr>
<td>RP mismatch</td>
<td>Number of PIM control packets received for which the routing device has an RP mismatch.</td>
</tr>
</tbody>
</table>
### Table 121: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP mode mismatch</td>
<td>RP mode (sparse or bidirectional) mismatches encountered when processing join and prune messages.</td>
</tr>
<tr>
<td>RPF neighbor unknown</td>
<td>Number of PIM control packets received for which the routing device has an unknown RPF neighbor for the source.</td>
</tr>
<tr>
<td>Rx Joins/Prunes filtered</td>
<td>The number of join and prune messages filtered because of configured route filters and source address filters.</td>
</tr>
<tr>
<td>Tx Joins/Prunes filtered</td>
<td>The number of join and prune messages filtered because of configured route filters and source address filters.</td>
</tr>
<tr>
<td>Embedded-RP invalid addr</td>
<td>Number of packets received with an invalid embedded RP address in PIM join messages and other types of messages sent between routing domains.</td>
</tr>
<tr>
<td>Embedded-RP limit exceed</td>
<td>Number of times the limit configured with the <code>maximum-rps</code> statement is exceeded. The <code>maximum-rps</code> statement limits the number of embedded RPs created in a specific routing instance. The range is from 1 through 500. The default is 100.</td>
</tr>
<tr>
<td>Embedded-RP added</td>
<td>Number of packets in which the embedded RP for IPv6 is added. The following receive events trigger extraction of an IPv6 embedded RP address on the routing device:</td>
</tr>
<tr>
<td></td>
<td>• Multicast Listener Discovery (MLD) report for an embedded RP multicast group address</td>
</tr>
<tr>
<td></td>
<td>• PIM join message with an embedded RP multicast group address</td>
</tr>
<tr>
<td></td>
<td>• Static embedded RP multicast group address associated with an interface</td>
</tr>
<tr>
<td></td>
<td>• Packets sent to an embedded RP multicast group address received on the DR</td>
</tr>
<tr>
<td></td>
<td>An embedded RP node discovered through these receive events is added if it does not already exist on the routing platform.</td>
</tr>
<tr>
<td>Embedded-RP removed</td>
<td>Number of packets in which the embedded RP for IPv6 is removed. The embedded RP is removed whenever all PIM join states using this RP are removed or the configuration changes to remove the embedded RP feature.</td>
</tr>
<tr>
<td>Rx Register msgs filtering</td>
<td>Number of received register messages dropped because of a filter configured for PIM register messages.</td>
</tr>
<tr>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>Tx Register msgs filtering</td>
<td>Number of register messages dropped because of a filter configured for PIM register messages.</td>
</tr>
<tr>
<td>drop</td>
<td></td>
</tr>
<tr>
<td>Rx Bidir Join/Prune on non-Bidir if</td>
<td>Error counter for join and prune messages received on non-bidirectional PIM interfaces.</td>
</tr>
</tbody>
</table>
### Table 12: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Bidir Join/Prune on non-DF if</td>
<td>Error counter for join and prune messages received on non-designated forwarder interfaces.</td>
</tr>
<tr>
<td>V4 (S,G) Maximum</td>
<td>Maximum number of (S,G) IPv4 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.</td>
</tr>
<tr>
<td>V4 (S,G) Accepted</td>
<td>Number of accepted (S,G) IPv4 multicast routes.</td>
</tr>
<tr>
<td>V4 (S,G) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv4 multicast routes accepted by the device).</td>
</tr>
<tr>
<td>V4 (S,G) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 (S,G) Maximum</td>
<td>Maximum number of (S,G) IPv6 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.</td>
</tr>
<tr>
<td>V6 (S,G) Accepted</td>
<td>Number of accepted (S,G) IPv6 multicast routes.</td>
</tr>
<tr>
<td>V6 (S,G) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv6 multicast routes accepted by the device).</td>
</tr>
<tr>
<td>V6 (S,G) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Maximum</td>
<td>Maximum number of group-to-rendezvous point (RP) IPv4 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Accepted</td>
<td>Number of accepted group-to-RP IPv4 multicast mappings.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv4 multicast mappings accepted by the device).</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Maximum</td>
<td>Maximum number of group-to RP IPv6 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Accepted</td>
<td>Number of accepted group-to-RP IPv6 multicast mappings.</td>
</tr>
</tbody>
</table>
Table 121: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V6 (grp-prefix, RP) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv6 multicast mappings accepted by the device).</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V4 Register Maximum</td>
<td>Maximum number of IPv4 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.</td>
</tr>
<tr>
<td>V4 Register Accepted</td>
<td>Number of accepted IPv4 PIM registers.</td>
</tr>
<tr>
<td>V4 Register Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of IPv4 PIM registers accepted by the device).</td>
</tr>
<tr>
<td>V4 Register Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 Register Maximum</td>
<td>Maximum number of IPv6 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.</td>
</tr>
<tr>
<td>V6 Register Accepted</td>
<td>Number of accepted IPv6 PIM registers.</td>
</tr>
<tr>
<td>V6 Register Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of IPv6 PIM registers accepted by the device).</td>
</tr>
<tr>
<td>V6 Register Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>(*,G) Join drop due to SSM range check</td>
<td>PIM join messages that are dropped because the multicast addresses are outside of the SSM address range of 232.0.0.0 through 232.255.255.255. You can extend the accepted SSM address range by configuring the ssm-groups statement.</td>
</tr>
</tbody>
</table>

Sample Output

show pim statistics

```
user@host> show pim statistics

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>15</td>
<td>32</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>362</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>483</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>18</td>
<td>518</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Graft</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
</tr>
<tr>
<td>V2 State Refresh</td>
<td>0</td>
</tr>
<tr>
<td>V2 DF Election</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
</tr>
</tbody>
</table>

**Global Statistics**

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello dropped on neighbor policy</td>
<td>0</td>
</tr>
<tr>
<td>Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>V1 Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>Unknown Version</td>
<td>0</td>
</tr>
<tr>
<td>ipv4 BSR pkt drop due to excessive rate</td>
<td>0</td>
</tr>
<tr>
<td>ipv6 BSR pkt drop due to excessive rate</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor unknown</td>
<td>0</td>
</tr>
<tr>
<td>Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>0</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Data</td>
<td>0</td>
</tr>
<tr>
<td>Rx Intf disabled</td>
<td>0</td>
</tr>
<tr>
<td>Rx V1 Require V2</td>
<td>0</td>
</tr>
<tr>
<td>Rx V2 Require V1</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register not RP</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register no route</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register no decap if</td>
<td>0</td>
</tr>
<tr>
<td>Null Register Timeout</td>
<td>0</td>
</tr>
<tr>
<td>RP Filtered Source</td>
<td>0</td>
</tr>
<tr>
<td>Rx Unknown Reg Stop</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune upstream if</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune for invalid group</td>
<td>5</td>
</tr>
<tr>
<td>Rx Join/Prune messages dropped</td>
<td>0</td>
</tr>
<tr>
<td>Rx sparse join for dense group</td>
<td>0</td>
</tr>
<tr>
<td>Rx Craft/Graft Ack no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx Craft on upstream if</td>
<td>0</td>
</tr>
<tr>
<td>Rx CRP not BSR</td>
<td>0</td>
</tr>
<tr>
<td>Rx BSR when BSR</td>
<td>0</td>
</tr>
<tr>
<td>Rx BSR not RPF if</td>
<td>0</td>
</tr>
<tr>
<td>Rx unknown hello opt</td>
<td>0</td>
</tr>
<tr>
<td>Rx data no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx RP no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx aggregate</td>
<td>0</td>
</tr>
<tr>
<td>Rx malformed packet</td>
<td>0</td>
</tr>
<tr>
<td>Rx illegal TTL</td>
<td>0</td>
</tr>
<tr>
<td>Rx illegal destination address</td>
<td>0</td>
</tr>
<tr>
<td>No RP</td>
<td>0</td>
</tr>
<tr>
<td>No register encap if</td>
<td>0</td>
</tr>
</tbody>
</table>
### Sample Output

**show pim statistics inet interface <interface-name>**

```bash
user@host> show pim statistics inet interface ge-0/3/0.0
```

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Sample Output

**show pim statistics inet6 interface <interface-name>**

```bash
user@host> show pim statistics inet6 interface ge-0/3/0.0
```

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show pim statistics instance <instance-name>

user@host> show pim statistics instance VPN-A

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>31</td>
<td>37</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>16</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 State Refresh</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 DF Election</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Global Statistics

- Hello dropped on neighbor policy: 0
- Unknown type: 0
- V1 Unknown type: 0
- Unknown Version: 0
- Neighbor unknown: 0
- Bad Length: 0
- Bad Checksum: 0
- Bad Receive If: 0
- Rx Bad Data: 0
- Rx Intf disabled: 0
- Rx V1 Require V2: 0
- Rx V2 Require V1: 0
- Rx Register not RP: 0
Rx Register no route                          0
Rx Register no decap if                       0
Null Register Timeout                         0
RP Filtered Source                            0
Rx Unknown Reg Stop                           0
Rx Join/Prune no state                        0
Rx Join/Prune on upstream if                  0
Rx Join/Prune for invalid group               0
Rx Join/Prune messages dropped                0
Rx sparse join for dense group                0
Rx Craft/Graft Ack no state                   0
Rx Craft on upstream if                       0
Rx CRP not BSR                                 0
Rx BSR when BSR                               0
Rx BSR not RPF if                             0
Rx unknown hello opt                          0
Rx data no state                              0
Rx RP no state                                0
Rx aggregate                                  0
Rx malformed packet                           0
Rx illegal TTL                                 0
Rx illegal destination address                0
No RP                                         0
No register encap if                          0
No route upstream                             28
Nexthop Unusable                              0
RP mismatch                                    0
RP mode mismatch                               0
RPF neighbor unknown                           0
Rx Joins/Prunes filtered                      0
Tx Joins/Prunes filtered                      0
Embedded-RP invalid addr                      0
Embedded-RP limit exceed                      0
Embedded-RP added                             0
Embedded-RP removed                           0
Rx Register msgs filtering drop               0
Tx Register msgs filtering drop               0
Rx Bidir Join/Prune on non-Bidir if           0
Rx Bidir Join/Prune on non-DF if              0
V4 (S,G) Maximum                              10
V4 (S,G) Accepted                             9
V4 (S,G) Threshold                            80
V4 (S,G) Log Interval                         80
V6 (S,G) Maximum                              8
V6 (S,G) Accepted                             8
V6 (S,G) Threshold                            50
V6 (S,G) Log Interval                         100
V4 (grp-prefix, RP) Maximum                   100
V4 (grp-prefix, RP) Accepted                  5
V4 (grp-prefix, RP) Threshold                 80
V4 (grp-prefix, RP) Log Interval              10
V6 (grp-prefix, RP) Maximum                   20
V6 (grp-prefix, RP) Accepted                  0
V6 (grp-prefix, RP) Threshold                 90
V6 (grp-prefix, RP) Log Interval              20
V4 Register Maximum                           100
V4 Register Accepted                          10
V4 Register Threshold                         80
V4 Register Log Interval                      10
V6 Register Maximum                           20
Sample Output

show pim statistics interface <interface-name>

```
user@host> show pim statistics interface ge-0/3/0.0

Instance: PIM.master Family: INET

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Instance: PIM.master Family: INET6

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show sap listen

Syntax

```
show sap listen
<brief | detail>
<logical-system (all | logical-system-name)>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display the addresses that the router is listening to in order to receive multicast Session Announcement Protocol (SAP) session announcements.

Options

```
one—Display standard information about the addresses that the router is listening to in order to receive multicast SAP session announcements.
brief | detail—(Optional) Display the specified level of output.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
```

Required Privilege

view

List of Sample Output

```
show sap listen on page 2031
show sap listen brief on page 2032
show sap listen detail on page 2032
```

Output Fields

Table 122 on page 2031 describes the output fields for the `show sap listen` 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>Group address</td>
<td>Address of the group that the local router is listening to for SAP messages.</td>
</tr>
<tr>
<td>Port</td>
<td>UDP port number used for SAP.</td>
</tr>
</tbody>
</table>
```

Sample Output

```
show sap listen

user@host> show sap listen

<table>
<thead>
<tr>
<th>Group address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.2.127.254</td>
<td>9875</td>
</tr>
<tr>
<td>239.255.255.255</td>
<td>9875</td>
</tr>
</tbody>
</table>
```
show sap listen brief

The output for the show sap listen brief command is identical to that for the show sap listen command. For sample output, see show sap listen on page 2031.

show sap listen detail

The output for the show sap listen detail command is identical to that for the show sap listen command. For sample output, see show sap listen on page 2031.
test msdp

Syntax

```
test msdp (dependent-peers prefix | rpf-peer originator)
    <instance instance-name>
    <logical-system (all | logical-system-name)>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 12.1 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Find Multicast Source Discovery Protocol (MSDP) peers.

Options

- **dependent-peers prefix**—Find downstream dependent MSDP peers.
- **rpf-peer originator**—Find the MSDP reverse-path-forwarding (RPF) peer for the originator.
- **instance instance-name**—(Optional) Find MSDP peers for the specified routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

- **view**

List of Sample Output

- **test msdp dependent-peers on page 2033**

Output Fields

- When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
test msdp dependent-peers

user@host> test msdp dependent-peers 10.0.0.1/24
```
CHAPTER 20

IPv6 Operational Commands

- clear ipv6 neighbors
- clear ipv6 router-advertisement
- show ipv6 neighbors
- show ipv6 router-advertisement
clear ipv6 neighbors

Syntax

```
clear ipv6 neighbors
<all>
< host hostname>
< interface interface-name>
< logical-system logical-system-name>
< tenant name>
< vpn vpn-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.3 for EX Series switches.
Command introduced in Junos OS Release 12.2 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Clear IPv6 neighbor cache information.

NOTE: On Junos OS Evolved, issuing the `clear ipv6 neighbors` command clears the cache for IPv6 neighbors in a reachable state.

Options

- `none`—Clear all IPv6 neighbor cache information.
- `all`—(Optional) Clear all IPv6 neighbor cache information.
- `host hostname`—(Optional) Clear the information for the specified IPv6 neighbors.
- `interface interface-name`—(Optional) Clear the information about IPv6 for the specified logical interface.
- `logical-system logical-system-name`—(Optional) Clear the IPv6 entries for the specified logical system; only available in the main router context.
- `tenant name`—(Optional) Clear the IPv6 entries for the specified tenant system; only available in the main router context.
- `vpn vpn-name`—(Optional) Clear entries in the IPv6 table for the specified virtual private network’s (VPN) routing table.

Required Privilege

- Level: `view`

Related Documentation

- `show ipv6 neighbors` on page 2039

List of Sample Output

- `clear ipv6 neighbors` on page 2037
Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ipv6 neighbors

user@host> clear ipv6 neighbors
**clear ipv6 router-advertisement**

**Syntax**
clear ipv6 router-advertisement
  <interface interface>
  <logical-system (all | logical-system-name)>

**Release Information**
Command introduced before Junos OS Release 7.4.

**Description**
Clear IPv6 router advertisement counters.

**Options**

- none—Clear IPv6 router advertisement counters for all interfaces.
- interface interface—(Optional) Clear IPv6 router advertisement counters for the specified interface.
- logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**
view

**Related Documentation**
- show ipv6 router-advertisement on page 2042

**List of Sample Output**
clear ipv6 router-advertisement on page 2038

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear ipv6 router-advertisement

user@host> clear ipv6 router-advertisement
**show ipv6 neighbors**

**Syntax**

```
show ipv6 neighbors
<flags>
<hostname host-name>
<interface interface-name>
<logical-system logical-system-name>
<reference-count count>
<tenant name>
<vpn vpn-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.3 for EX Series switches.
Command introduced in Junos OS Release 12.2 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
`flags`, `hostname`, `interface`, `logical-system`, `reference-count`, `tenant`, and `vpn` options added
in Junos OS Release 18.3.

**Description**

Display information about the IPv6 neighbor cache.

---

**NOTE:** Starting with Junos OS Release 16.1, `show ipv6 neighbors` command

does not display the underlying ifl information if enhanced-convergence

statement at `[edit irb unit unit-number]` hierarchy level and enhanced-ip

statement at `[edit chassis network-services]` hierarchy level is configured for

the destination interface IRB.

---

**Options**

- **none**—Display the entries in the IPv6 table.
- **flags**—(Optional) Display the flags set, if any.
- **hostname host-name**—(Optional) Display the hostname.
- **interface interface-name**—(Optional) Display information about IPv6 for the specified

  logical interface
- **logical-system logical-system-name**—(Optional) Display the IPv6 entries for the specified

  logical system; only available on the main router context.
- **reference-count count**—(Optional) Display the IPv6 next-hop reference count.
- **tenant name**—(Optional) Displays the IPv6 entries for the specified tenant system; only

  available in the main router context.
- **vpn vpn-name**—(Optional) Display entries in the IPv6 table for the specified virtual private

  network’s (VPN) routing table.
**Required Privilege**  
- `view`

**Related Documentation**  
- clear ipv6 neighbors on page 2036

**List of Sample Output**  
- show ipv6 neighbors on page 2040
- show ipv6 neighbors on page 2040

**Output Fields**  
Table 123 on page 2040 describes the output fields for the `show ipv6 neighbors` command. Output fields are listed in the approximate order in which they appear.

**Table 123: show ipv6 neighbors Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>Name of the IPv6 interface.</td>
</tr>
<tr>
<td>Linklayer Address</td>
<td>Link-layer address.</td>
</tr>
<tr>
<td>State</td>
<td>State of the link: up, down, incomplete, reachable, stale, or unreachable.</td>
</tr>
<tr>
<td>Exp</td>
<td>Number of seconds until the entry expires.</td>
</tr>
<tr>
<td>Rtr</td>
<td>Whether the neighbor is a routing device: yes or no.</td>
</tr>
<tr>
<td>Secure</td>
<td>Whether this entry was created using the Secure Neighbor Discovery (SEND) protocol: yes or no.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
</tbody>
</table>

**Sample Output**

`show ipv6 neighbors`

```
user@host> show ipv6 neighbors
IPv6 Address          Linklayer Address  State   Exp  Rtr  Secure
Interface
2001:db8:0:1:2a0:a514:0:24c 00:05:85:8f:8c:bd  stale  546 yes no
fe-1/2/0.1
fe80::2a0:a514:0:24c 00:05:85:8f:8c:bd  stale  258 yes no
fe-1/2/0.1
fe80::2a0:a514:0:64c 00:05:85:8f:8c:bd  stale  111 yes no
fe-1/2/1.5
fe80::2a0:a514:0:4c 00:05:85:8f:8c:bd  stale  327 yes no
fe-1/2/2.9
```

`show ipv6 neighbors`

The command displaying the underlying l2 ifl information when `enhanced-convergence` statement and `enhanced-ip` statement is not configured.
<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Linklayer Address</th>
<th>State</th>
<th>Exp Rtr</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>23::23:0:0:2</td>
<td>00:00:23:00:00:02</td>
<td>reachable</td>
<td>0</td>
<td>no</td>
</tr>
<tr>
<td>xe-2/2/0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The command not displaying the underlying l2if information when `enhanced-convergence` statement and `enhanced-ip` statement is configured.
### show ipv6 router-advertisement

**Syntax**
```
show ipv6 router-advertisement
<conflicts>
<interface interface>
<logical-system (all | logical-system-name)>
<prefix prefix/prefix length>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 12.2 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display information about IPv6 router advertisements, including statistics about messages sent and received on interfaces, and information received from advertisements from other routers.

**Options**
- **none**—Display all IPv6 router advertisement information for all interfaces.
- **conflicts**—(Optional) Display only the IPv6 router advertisement information that is conflicting.
- **interface interface**—(Optional) Display IPv6 router advertisement information for the specified interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **prefix prefix/prefix length**—(Optional) Display IPv6 router advertisement information for the specified prefix.

**Additional Information**
The display identifies conflicting information by enclosing the value the router is advertising in brackets.

**Required Privilege Level**
view

**Related Documentation**
- clear ipv6 router-advertisement on page 2038

**List of Sample Output**
- show ipv6 router-advertisement on page 2043
- show ipv6 router-advertisement conflicts on page 2044
- show ipv6 router-advertisement prefix on page 2044

**Output Fields**
Table 124 on page 2043 describes the output fields for the show ipv6 router-advertisement command. Output fields are listed in the approximate order in which they appear.
**Table 124: show ipv6 router-advertisement 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>
<tr>
<td>Advertisements sent</td>
<td>Number of router advertisements sent and the elapsed time since they were sent.</td>
</tr>
<tr>
<td>Solicits received</td>
<td>Number of solicitation messages received.</td>
</tr>
<tr>
<td>Advertisements received</td>
<td>Number of router advertisements received.</td>
</tr>
<tr>
<td>Advertisements from</td>
<td>Names of interfaces from which router advertisements have been received and the elapsed time since the last one was received.</td>
</tr>
<tr>
<td>Managed</td>
<td>Managed address configuration flag: 0 (stateless) or 1 (stateful).</td>
</tr>
<tr>
<td>Other configuration</td>
<td>Other stateful configuration flag: 0 (stateless) or 1 (stateful).</td>
</tr>
<tr>
<td>Reachable time</td>
<td>Time that a node identifies a neighbor as reachable after receiving a reachability confirmation, in milliseconds.</td>
</tr>
<tr>
<td>Default lifetime</td>
<td>Default lifetime, in seconds: from 0 seconds to 18.2 hours. A setting of 0 indicates that the router is not a default router.</td>
</tr>
<tr>
<td>Retransmit timer</td>
<td>Time between retransmitted Neighbor Solicitation messages, in milliseconds.</td>
</tr>
<tr>
<td>Current hop limit</td>
<td>Configured current hop limit.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Name and length of the prefix.</td>
</tr>
<tr>
<td>Valid lifetime</td>
<td>How long the prefix remains valid for onlink determination.</td>
</tr>
<tr>
<td>Preferred lifetime</td>
<td>How long the prefix generated by stateless autoconfiguration remains preferred.</td>
</tr>
<tr>
<td>On link</td>
<td>Onlink flag: 0 (not onlink) or 1 (onlink).</td>
</tr>
<tr>
<td>Autonomous</td>
<td>Autonomous address configuration flag: 0 (not autonomous) or 1 (autonomous).</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show ipv6 router-advertisement

user@host> show ipv6 router-advertisement
Interface: fe-0/1/1.0
    Advertisements sent: 0
    Solicits received: 0
    Advertisements received: 0
Interface: fxp0.0
    Advertisements sent: 0
    Solicits received: 0
```
show ipv6 router-advertisement conflicts

user@host> show ipv6 router-advertisement conflicts

Interface: fxp0.0
Advertisement from fe80::2d0:b7ff:fe1e:7b0e, heard 00:01:08 ago
Other configuration: 0 [1]

show ipv6 router-advertisement prefix

user@host> show ipv6 router-advertisement prefix 2001:db8:8040::/16

Interface: fe-0/1/3.0
Advertisements sent: 3, last sent 00:04:11 ago
Solicits received: 0
Advertisements received: 3
Advertisement from fe80::290:69ff:fe9a:5403, heard 00:00:05 ago
Managed: 0
Other configuration: 0
Reachable time: 0 ms
Default lifetime: 180 sec [1800 sec]
Retransmit timer: 0 ms
Current hop limit: 64
Prefix: 2001:db8:8040::/64
Valid lifetime: 2592000 sec
Preferred lifetime: 604800 sec
On link: 1
Autonomous: 1
CHAPTER 21

IS-IS Operational Commands

- clear isis adjacency
- clear isis database
- clear isis overload
- clear isis statistics
- show isis adjacency
- show isis authentication
- show isis backup coverage
- show isis backup label-switched-path
- show isis backup spf results
- show isis context-identifier
- show isis database
- show isis hostname
- show isis interface
- show isis overview
- show isis route
- show isis spf
- show isis statistics
clear isis adjacency

List of Syntax  Syntax on page 2046  Syntax (EX Series Switches and QFX Series) on page 2046

Syntax  clear isis adjacency
<all>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
<neighbor>

Syntax (EX Series Switches and QFX Series)  clear isis adjacency
<all>
<instance instance-name>
<interface interface-name>
<neighbor>

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 12.1 for the QFX Series.
all option introduced in Junos OS Release 14.2.

Description  Remove entries from the IS-IS adjacency database.

Options  all—Remove all entries from the adjacency database.

  instance instance-name—(Optional) Clear all adjacencies for the specified routing instance only.

  interface interface-name—(Optional) Clear all adjacencies for the specified interface only.

  logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

  neighbor—(Optional) Clear adjacencies for the specified neighbor only.

Required Privilege Level  clear

Related Documentation  • show isis adjacency on page 2054

List of Sample Output  clear isis adjacency on page 2047  clear isis adjacency all on page 2047
Output Fields

See show isis adjacency for an explanation of output fields.

Sample Output

clear isis adjacency

The following sample output displays IS-IS adjacency database information before and after the clear isis adjacency command is entered:

```
user@host> show isis adjacency
IS-IS adjacency database:
Interface System L State Hold (secs) SNPA
so-1/0/0.0 karakul 3 Up 26
so-1/1/3.0 1921.6800.5080 3 Up 23
so-5/0/0.0 1921.6800.5080 3 Up 19

user@host> clear isis adjacency karakul

user@host> show isis adjacency
IS-IS adjacency database:
Interface System L State Hold (secs) SNPA
so-1/0/0.0 karakul 3 Initializing 26
so-1/1/3.0 1921.6800.5080 3 Up 24
so-5/0/0.0 1921.6800.5080 3 Up 21
```

clear isis adjacency all

```
user@host> clear isis adjacency all

IS-IS adjacency database:
Interface System L State Hold (secs) SNPA
so-1/0/0.0 karakul 3 Initializing 26
so-1/1/3.0 1921.6800.5080 3 Initializing 24
so-5/0/0.0 1921.6800.5080 3 Initializing 21
```
clear isis database

List of Syntax  Syntax on page 2048
  Syntax (EX Series Switches and QFX Series) on page 2048

Syntax  clear isis database
  <all>
  <entries>
  <instance instance-name>
  <logical-system (all | logical-system-name)> 

Syntax (EX Series Switches and QFX Series)  clear isis database
  <all>
  <entries>
  <instance instance-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 12.1 for the QFX Series.
  Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
  Command introduced in 15.1X53-D30 for QFX10002 switch.

Description  Remove the entries from the IS-IS link-state database, which contains prefixes and topology information.

Options  all—Remove all entries from the IS-IS link-state database for all routing instances.

  entries—(Optional) Name of the database entry.

  instance instance-name—(Optional) Clear all entries for the specified routing instance.

  logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level  clear

Related Documentation  • show isis database on page 2071

List of Sample Output  clear isis database on page 2049

Output Fields  See show isis database for an explanation of output fields.
## Sample Output

clear isis database

The following sample output displays IS-IS link-state database information before and after the `clear isis database all` command is entered:

```
user@host> show isis database
IS-IS level 1 link-state database:
<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>crater.00-00</td>
<td>0x12</td>
<td>0x84dd</td>
<td>1139</td>
</tr>
</tbody>
</table>
1 LSPs

IS-IS level 2 link-state database:
<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>crater.00-00</td>
<td>0x19</td>
<td>0xe92c</td>
<td>1134</td>
</tr>
<tr>
<td>badlands.00-00</td>
<td>0x16</td>
<td>0x1454</td>
<td>985</td>
</tr>
<tr>
<td>carlsbad.00-00</td>
<td>0x33</td>
<td>0x220b</td>
<td>1015</td>
</tr>
<tr>
<td>ranier.00-00</td>
<td>0x2e</td>
<td>0xfc31</td>
<td>1007</td>
</tr>
<tr>
<td>1921.6800.5066.00-00</td>
<td>0x11</td>
<td>0x7313</td>
<td>566</td>
</tr>
<tr>
<td>1921.6800.5067.00-00</td>
<td>0x14</td>
<td>0xd9d4</td>
<td>939</td>
</tr>
</tbody>
</table>
6 LSPs

user@host> clear isis database all

user@host> show isis database
```

IS-IS level 1 link-state database:
<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime (secs)</th>
</tr>
</thead>
</table>

IS-IS level 2 link-state database:
<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime (secs)</th>
</tr>
</thead>
</table>
### clear isis overload

**List of Syntax**

Syntax on page 2050  
Syntax (EX Series Switches and QFX Series) on page 2050

**Syntax**

- clear isis overload  
  - `<instance instance-name>`  
  - `<logical-system (all | logical-system-name)>`

**Syntax (EX Series Switches and QFX Series)**

- clear isis overload  
  - `<instance instance-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 12.1 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Reset the IS-IS dynamic overload bit. This command can appear to not work, continuing to display overload after execution. The bit is reset only if the root cause is corrected by configuration remotely or locally.

When other routers detect that the overload bit is set, they do not use this routing device for transit traffic, but they do use it for packets destined to the overloaded routing device's directly connected networks and IP prefixes.

**Options**

- **none**—Reset the IS-IS dynamic overload bit.  
  - `instance instance-name`—(Optional) Reset the IS-IS dynamic overload bit for the specified routing instance.  
  - `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

- clear

**Related Documentation**

- show isis database on page 2071

**List of Sample Output**

- clear isis overload on page 2051

**Output Fields**

See show isis database for an explanation of output fields.
Sample Output

`clear isis overload`

The following sample output displays IS-IS database information before and after the `clear isis overload` command is entered:

```
user@host> show isis database
IS-IS level 1 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
pro3-c.00-00                     0x4   0x10db     1185 L1 L2 Overload
  1 LSPs
IS-IS level 2 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
pro3-c.00-00                     0x5   0x429f     1185 L1 L2 Overload
pro2-a.00-00                   0x91e   0x2589      874 L1 L2
pro2-a.02-00                     0x1    0xcbc      874 L1 L2
  3 LSPs

user@host> clear isis overload

user@host> show isis database
IS-IS level 1 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
pro3-c.00-00                     0xa   0x429e     1183 L1 L2
  1 LSPs
IS-IS level 2 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
pro3-c.00-00                     0xc   0x9c39     1183 L1 L2
pro2-a.00-00                   0x91e   0x2589      783 L1 L2
pro2-a.02-00                     0x1    0xcbc      783 L1 L2
  3 LSPs
```
clear isis statistics

**List of Syntax**  
Syntax on page 2052  
Syntax (EX Series Switches and QFX Series) on page 2052

**Syntax**  
```plaintext
clear isis statistics  
<instance instance-name>  
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**  
```plaintext
clear isis statistics  
<instance instance-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 12.1 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**  
Set statistics about IS-IS traffic to zero.

**Options**  
none—Set IS-IS traffic statistics to zero for all routing instances.

instance instance-name—(Optional) Set IS-IS traffic statistics to zero for the specified routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**  
view

**Related Documentation**  
• show isis statistics on page 2107

**List of Sample Output**  
clear isis statistics on page 2052

**Output Fields**  
See show isis statistics for an explanation of output fields.

**Sample Output**

### clear isis statistics

The following sample output displays IS-IS statistics before and after the clear isis statistics command is entered:

```plaintext
user@host> show isis statistics
```
IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>12793</td>
<td>12793</td>
<td>0</td>
<td>8666</td>
<td>719</td>
</tr>
<tr>
<td>IIH</td>
<td>116751</td>
<td>116751</td>
<td>0</td>
<td>118834</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>203956</td>
<td>203956</td>
<td>0</td>
<td>204080</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>7356</td>
<td>7350</td>
<td>6</td>
<td>8635</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>340856</td>
<td>340850</td>
<td>6</td>
<td>340215</td>
<td>719</td>
</tr>
</tbody>
</table>

Total packets received: 340856 Sent: 340934

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 1064
Fragments rebuilt: 1087
LSP regenerations: 436
Purges initiated: 0

user@host> clear isis statistics

user@host> show isis statistics

IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IIH</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

Total packets received: 5 Sent: 7

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 0
Fragments rebuilt: 0
LSP regenerations: 0
Purges initiated: 0
show isis adjacency

List of Syntax
Syntax (EX Series Switches and QFX Series) on page 2054

Syntax

show isis adjacency
<system-id>
<brief | detail | extensive>
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)

show isis adjacency
<system-id>
<brief | detail | extensive>
<instance instance-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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Display information about IS-IS neighbors.

Options
none—Display standard information about IS-IS neighbors for all routing instances.

system id—(Optional) Display information about IS-IS neighbors for the specified intermediate system.

brief | detail | extensive—(Optional) Display standard information about IS-IS neighbors with the specified level of output.

instance instance-name—(Optional) Display information about IS-IS neighbors for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Display information about IS-IS neighbors for all logical systems or for a particular logical system.

Required Privilege
Level
view

Related Documentation
• clear isis adjacency on page 2046

List of Sample Output
show isis adjacency on page 2057
show isis adjacency brief on page 2057
show isis adjacency detail on page 2058
show isis adjacency extensive on page 2058
Output Fields  
Table 125 on page 2055 describes the output fields for the `show isis adjacency` command. Output fields are listed in the approximate order in which they appear.

Table 125: show isis adjacency 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 through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>System</td>
<td>System identifier (sysid), displayed as a name, if possible.</td>
<td>brief</td>
</tr>
<tr>
<td>L or Level</td>
<td>Level:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An exclamation point (!) preceding the level number indicates that the adjacency is missing an IP address.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>State of the adjacency: Up, Down, New, One-way, Initializing, or Rejected.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold (secs)</td>
<td>Remaining hold time of the adjacency.</td>
<td>brief</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
<td>brief</td>
</tr>
<tr>
<td>Expires in</td>
<td>How long the adjacency expires, in seconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority to become the designated intermediate system.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Up/Down transitions</td>
<td>Count of adjacency status changes from Up to Down or from Down to Up.</td>
<td>detail</td>
</tr>
<tr>
<td>Last transition</td>
<td>Time of the last Up/Down transition.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit type</td>
<td>Bit mask of levels on this interface: 1=Level 1 router; 2=Level 2 router; 3=both Level 1 and Level 2 router.</td>
<td>detail</td>
</tr>
<tr>
<td>Speaks</td>
<td>Protocols supported by this neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Topologies</td>
<td>Supported topologies.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Restart capable</td>
<td>Whether a neighbor is capable of graceful restart: Yes or No.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Adjacency</td>
<td>This routing device has signaled to advertise this interface to its neighbors in their link-state PDUs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>advertisement:</td>
<td>Advertise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This neighbor has signaled not to advertise the interface in the routing device's outbound link-state PDUs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suppress</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc. 2055
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP addresses</td>
<td>IP address of this neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>IPV6 Address</td>
<td>IPv6 address of the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Level 1 IPv4 Adj-SID</td>
<td>Level 1 IPv4 node-SID of the adjacent neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Level 1 IPv6 Adj-SID</td>
<td>Level 1 IPv6 node-SID of the adjacent neighbor.</td>
<td></td>
</tr>
<tr>
<td>Level 2 IPv4 Adj-SID</td>
<td>Level 2 IPv4 node-SID of the adjacent neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Level 2 IPv6 Adj-SID</td>
<td>Level 2 IPv6 node-SID of the adjacent neighbor.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 125: show isis adjacency Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition log</td>
<td>List of recent transitions, including:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• When—Time at which an IS-IS adjacency transition occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—Current state of the IS-IS adjacency (up, down, or rejected).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Up—Adjacency is up and operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Adjacency is down and not available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rejected—Adjacency has been rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event—Type of transition that occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Seenself—Possible routing loop has been detected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface down—IS-IS interface has gone down and is no longer available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Error—Adjacency error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down reason—Reason that an IS-IS adjacency is down:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3-Way Handshake Failed—Connection establishment failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Address Mismatch—Address mismatch caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aged Out—Link expired.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISO Area Mismatch—IS-IS area mismatch caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad Hello—Unacceptable hello message caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BFD Session Down—Bidirectional failure detection caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Disabled—IS-IS interface is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Down—IS-IS interface is unavailable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Level Disabled—IS-IS level is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Level Changed—IS-IS level has changed on the adjacency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Level Mismatch—Levels on adjacency are not compatible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MPLS LSP Down—Label-switched path (LSP) is unavailable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MT Topology Changed—IS-IS topology has changed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MT Topology Mismatch—IS-IS topology is mismatched.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote System ID Changed—Adjacency peer system ID changed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Protocol Shutdown—IS-IS protocol is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CLI Command—Adjacency brought down by user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unknown—Unknown.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show isis adjacency

```
user@host> show isis adjacency
Interface             System         L State        Hold (secs) SNPA
at-2/3/0.0            ranier         3  Up                   23
```

show isis adjacency brief

The output for the show isis adjacency brief command is identical to that for the show isis adjacency command. For sample output, see show isis adjacency on page 2057.
show isis adjacency detail

user@host> show isis adjacency detail

ranier
  Interface: at-2/3/0.0, Level: 3, State: Up, Expires in 21 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 00:01:09 ago
  Circuit type: 3, Speaks: IP, IPv6
  Topologies: Unicast, IPV6-Unicast  Restart capable: Yes, Adjacency advertisement: Advertise
  LAN id: pro-bng3-c-F.02, IP addresses: 11.1.1.2
  IPv6 addresses: fe80::2a0:a514:0:4745
  Level 1 IPv4 Adj-SID: 299808, IPv6 Adj-SID: 299824

show isis adjacency extensive

user@host> show isis adjacency extensive

ranier
  Interface: at-2/3/0.0, Level: 3, State: Up, Expires in 22 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 00:01:16 ago
  Circuit type: 3, Speaks: IP, IPv6
  Topologies: Unicast, IPV6-Unicast
  Restart capable: Yes, Adjacency advertisement: Advertise
  IP addresses: 11.1.1.2
  IPv6 addresses: fe80::2a0:a514:0:3e45
  Level 1 IPv4 Adj-SID: 300112, IPv6 Adj-SID: 300304
  Level 2 IPv4 Adj-SID: 300320, IPv6 Adj-SID: 300336
  Transition log:
    When                  State        Event           Down reason
    Thu Mar 26 06:13:18   Up           Seenself
show isis authentication

List of Syntax  Syntax on page 2059
Syntax (EX Series Switches and QFX Series) on page 2059

Syntax  show isis authentication
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)  show isis authentication
<instance instance-name>

Release Information  Command introduced in Junos OS Release 7.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Support for hitless authentication key rollover introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.


Options  none—Display information about IS-IS authentication.

instance instance-name—(Optional) Display IS-IS authentication for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege  view

Related Documentation  • show security keychain

List of Sample Output  show isis authentication on page 2060
show isis authentication (With Hitless Authentication Key Rollover Configured) on page 2060

Output Fields  Table 126 on page 2060 describes the output fields for the show isis authentication command. Output fields are listed in the approximate order in which they appear.
### Table 126: `show isis authentication` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>Level</td>
<td>IS-IS level.</td>
</tr>
<tr>
<td>IIH Auth</td>
<td>IS-IS Hello (IIH) packet authentication type.</td>
</tr>
<tr>
<td></td>
<td>Displays the name of the active keychain if hitless authentication key rollover is configured.</td>
</tr>
<tr>
<td>CSN Auth</td>
<td>Complete sequence number authentication type.</td>
</tr>
<tr>
<td>PSN Auth</td>
<td>Partial sequence number authentication type.</td>
</tr>
<tr>
<td>L1 LSP Authentication</td>
<td>Layer 1 link-state PDU authentication type.</td>
</tr>
<tr>
<td>L2 LSP Authentication</td>
<td>Layer 2 link-state PDU authentication type.</td>
</tr>
</tbody>
</table>

### Sample Output

**show isis authentication**

```
user@host> show isis authentication

<table>
<thead>
<tr>
<th>Interface</th>
<th>Level</th>
<th>IIH Auth</th>
<th>CSN Auth</th>
<th>PSN Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-2/3/0.0</td>
<td>1</td>
<td>Simple</td>
<td>Simple</td>
<td>Simple</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Simple</td>
<td>Simple</td>
<td>Simple</td>
</tr>
</tbody>
</table>

L1 LSP Authentication: Simple
L2 LSP Authentication: MD5
```

**show isis authentication (With Hitless Authentication Key Rollover Configured)**

```
user@host> show isis authentication

<table>
<thead>
<tr>
<th>Interface</th>
<th>Level</th>
<th>IIH Auth</th>
<th>CSN Auth</th>
<th>PSN Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/1/3.0</td>
<td>2</td>
<td>hakrhello</td>
<td>MD5</td>
<td>MD5</td>
</tr>
</tbody>
</table>

L2 LSP Authentication: MD5
```
show isis backup coverage

Syntax
show isis backup coverage
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)
show isis backup coverage
<instance instance-name>

Release Information
Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Display information about the level of backup coverage available.

Options
none — Display information about the level of backup coverage available for all the nodes and prefixes in the network.

instance instance-name — (Optional) Display information about the level of backup coverage for a specific IS-IS routing instance.

logical-system (all | logical-system-name) — (Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level
view

Related Documentation
• Understanding Loop-Free Alternate Routes for IS-IS
• Example: Configuring Node-Link Protection for IS-IS Routes in a Layer 3 VPN
• show isis backup label-switched-path on page 2063

List of Sample Output
show isis backup coverage on page 2062

Output Fields
Table 127 on page 2061 lists the output fields for the show isis backup coverage command. Output fields are listed in the approximate order in which they appear.

Table 127: show isis backup coverage Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Type of topology or address family: IPV4 Unicast or IPV6 Unicast.</td>
</tr>
</tbody>
</table>
### Table 127: show isis backup coverage Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td>IS-IS level:</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1</td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2</td>
</tr>
<tr>
<td><strong>Node</strong></td>
<td>By topology, the percentage of all routes configured on the node that are protected through backup coverage.</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td>Percentage of IPv4 unicast routes that are protected through backup coverage.</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td>Percentage of IPv6 unicast routes that are protected through backup coverage.</td>
</tr>
<tr>
<td><strong>CLNS</strong></td>
<td>Percentage of Connectionless Network Service (CLNS) routes that are protected through backup coverage.</td>
</tr>
</tbody>
</table>

### Sample Output

**show isis backup coverage**

```plaintext
user@host> show isis backup coverage
Backup Coverage:
Topology    Level    Node    IPv4    IPv6    CLNS
IPV4 Unicast 2 28.57% 22.22% 0.00% 0.00%
IPV6 Unicast 2 0.00% 0.00% 0.00% 0.00%
```
**show isis backup label-switched-path**

**Syntax**
```
show isis backup label-switched-path
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**
```
show isis backup label-switched-path
```

**Release Information**
Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display information about MPLS label-switched-paths (LSPs) designated as backup routes for IS-IS routes.

**Options**
- **none**—Display information about MPLS LSPs designated as backup routes for IS-IS routes.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**Related Documentation**
- Understanding Loop-Free Alternate Routes for IS-IS
- Example: Configuring Node-Link Protection for IS-IS Routes in a Layer 3 VPN
- show isis backup coverage on page 2061

**List of Sample Output**
show isis backup label-switched-path on page 2064

**Output Fields**
`Table 128 on page 2063` lists the output fields for the `show isis backup label-switched-path` 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>Backup MPLS LSPs</td>
<td>List of MPLS LSPs designated as backup paths for IS-IS routes.</td>
</tr>
<tr>
<td>Egress</td>
<td>IP address of the egress routing device for the LSP.</td>
</tr>
</tbody>
</table>
Table 128: show isis backup label-switched-path Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>State of the LSP:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Up</strong>—The routing device can detect RSVP hello messages from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—The routing device has received one of the following indications:</td>
</tr>
<tr>
<td></td>
<td>• Communication failure from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Communication from IGP that the neighbor is unavailable.</td>
</tr>
<tr>
<td></td>
<td>• Change in the sequence numbers in the RSVP hello messages sent by the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deleted</strong>—LSP is no longer available as a backup path.</td>
</tr>
<tr>
<td>Last change</td>
<td>Time elapsed since the neighbor state changed either from up to down or from down to up. The format is $hh:mm:ss$.</td>
</tr>
<tr>
<td>TE-metric</td>
<td>Configured traffic engineering metric.</td>
</tr>
<tr>
<td>Metric</td>
<td>Configured metric.</td>
</tr>
</tbody>
</table>

Sample Output

show isis backup label-switched-path

```
user@host> show isis backup label-switched-path
Backup MPLS LSPs:
f-to-g, Egress: 192.168.1.4, Status: up, Last change: 06:12:03
  TE-metric: 9, Metric: 0
```
## show isis backup spf results

**Syntax**

```
show isis backup spf results
<instance instance-name>
<level (1 | 2)>
<logical-system (all | logical-system-name)>
<no-coverage>
<topology (ipv4-unicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**Syntax (EX Series Switches)**

```
show isis backup spf results
<instance instance-name>
<level (1 | 2)>
<no-coverage>
<topology (ipv4-unicast | unicast)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.

**Description**

Display information about IS-IS shortest-path-first (SPF) calculations for backup paths.

**Options**

- **none**—Display information about IS-IS SPF calculations for all backup paths for all destination nodes.
  - **instance instance-name**—(Optional) Display SPF calculations for backup paths for the specified routing instance.
  - **level (1 | 2)**—(Optional) Display SPF calculations for the backup paths for the specified IS-IS level.
  - **logical-system logical-system-name**—(Optional) Display SPF calculations for the backup paths for all logical systems or on a particular logical system.
  - **no-coverage**—(Optional) Display SPF calculations only for destinations that do not have backup coverage.
  - **topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)**—(Optional) Display SPF calculations for backup paths for the specified topology only.

**Required Privilege**

view

**Related Documentation**

- Example: Configuring Link and Node Protection for IS-IS Routes
- show isis backup coverage on page 2061
- Understanding Loop-Free Alternate Routes for IS-IS
- Example: Configuring Node-Link Protection for IS-IS Routes in a Layer 3 VPN
List of Sample Output  
show isis backup spf results on page 2066
show isis backup spf results no-coverage on page 2067

Output Fields  
Table 129 on page 2066 lists the output fields for the show isis backup spf results 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>node-name</td>
<td>Name of the destination node.</td>
</tr>
<tr>
<td>Address</td>
<td>Address of the destination node.</td>
</tr>
<tr>
<td>Primary next-hop</td>
<td>Interface and name of the node of the primary next hop to reach the destination.</td>
</tr>
<tr>
<td>Root</td>
<td>Name of the next-hop neighbor.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric to the node.</td>
</tr>
<tr>
<td>Eligible</td>
<td>Indicates that the next-hop neighbor has been designated as a backup path to the destination.</td>
</tr>
<tr>
<td>Backup next-hop</td>
<td>Name of the interface of the backup next hop.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
</tr>
<tr>
<td>LSP</td>
<td>Name of the MPLS label-switched path (LSP) designated as a backup path.</td>
</tr>
<tr>
<td>Not eligible</td>
<td>Indicates that the next-hop neighbor cannot function as a backup path to the destination.</td>
</tr>
<tr>
<td>Reason</td>
<td>Describes why the next-hop neighbor is designated as Not eligible as a backup path.</td>
</tr>
</tbody>
</table>

Sample Output  
show isis backup spf results

```
user@host> show isis backup spf results

IS-IS level 1 SPF results:
  0 nodes

IS-IS level 2 SPF results:
banff.00
  Primary next-hop: so-6/0/0.0, IPV4, olympic
  Primary next-hop: ae0.0, IPV4, camaro, SNPA: 0:90:69:f:67:f0
  Primary next-hop: so-6/0/0.0, IPV6, olympic
  Primary next-hop: ae0.0, IPV6, camaro, SNPA: 0:90:69:f:67:f0
  Root: camaro, Root Metric: 10, Metric: 10
```
Not eligible, Reason: Primary next-hop multipath
Root: olympic, Root Metric: 10, Metric: 10
Not eligible, Reason: Primary next-hop multipath
Root: glacier, Root Metric: 10, Metric: 25
Not eligible, Reason: Primary next-hop multipath

Primary next-hop: so-6/0/0.0, IPV4, olympic
Primary next-hop: so-6/0/0.0, IPV6, olympic
Root: olympic, Root Metric: 10, Metric: 10
Not eligible, Reason: Primary next-hop link fate sharing
Root: glacier, Root Metric: 10, Metric: 15
Eligible, Backup next-hop: as0.0, IPV4, glacier
Eligible, Backup next-hop: as0.0, IPV6, glacier
Root: camaro, Root Metric: 10, Metric: 20
Not eligible, Reason: Interface is already covered

Primary next-hop: so-6/0/0.0, IPV4, olympic
Primary next-hop: so-6/0/0.0, IPV6, olympic
Root: olympic, Root Metric: 10, Metric: 0
Not eligible, Reason: Primary next-hop link fate sharing
Root: camaro, Root Metric: 10, Metric: 20
track-item: olympic.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops
Root: glacier, Root Metric: 10, Metric: 20
track-item: olympic.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops

Primary next-hop: ae0.0, IPV4, camaro, SNPA: 0:90:69:f:67:f0
Primary next-hop: ae0.0, IPV6, camaro, SNPA: 0:90:69:f:67:f0
Root: camaro, Root Metric: 10, Metric: 0
Not eligible, Reason: Primary next-hop link fate sharing
Root: glacier, Root Metric: 10, Metric: 20
track-item: camaro.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops
Root: olympic, Root Metric: 10, Metric: 20
track-item: camaro.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops

Primary next-hop: as0.0, IPV4, glacier
Primary next-hop: as0.0, IPV6, glacier
Root: glacier, Root Metric: 10, Metric: 0
Not eligible, Reason: Primary next-hop link fate sharing
Root: camaro, Root Metric: 10, Metric: 20
track-item: glacier.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops
Root: olympic, Root Metric: 10, Metric: 20
track-item: glacier.00-00
track-item: kobuk.00-00
Not eligible, Reason: Path loops

5 nodes
IS-IS level 1 SPF results:
pro-bng3-k.00
  Primary next-hop: fe-1/3/3.0, IPV4, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
  Primary next-hop: fe-1/3/3.0, IPV6, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
  Root: pro-bng3-k, Root Metric: 10, Metric: 0, Root Preference: 0x0
  track-item: pro-bng3-j.00-00
  track-item: pro-bng3-i.00-00
pro-bng3-i.00
  Primary next-hop: fe-0/1/2.0, IPV4, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
  Primary next-hop: fe-0/1/2.0, IPV6, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
  Root: pro-bng3-i, Root Metric: 10, Metric: 0, Root Preference: 0x0
  track-item: pro-bng3-j.00-00
  track-item: pro-bng3-i.00-00

2 nodes

IS-IS level 2 SPF results:
olympic.00
  Primary next-hop: so-6/0/0.0, IPV4, olympic
  Primary next-hop: so-6/0/0.0, IPV6, olympic
  Root: olympic, Root Metric: 10, Metric: 0
  Not eligible, Reason: Primary next-hop link fate sharing
  track-item: olympic.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops
  track-item: olympic.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops
camaro.00
  Primary next-hop: ae0.0, IPV4, camaro, SNPA: 0:90:69:f:67:f0
  Primary next-hop: ae0.0, IPV6, camaro, SNPA: 0:90:69:f:67:f0
  Root: camaro, Root Metric: 10, Metric: 0
  Not eligible, Reason: Primary next-hop link fate sharing
  track-item: camaro.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops
  track-item: camaro.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops
glacier.00
  Primary next-hop: as0.0, IPV4, glacier
  Primary next-hop: as0.0, IPV6, glacier
  Root: glacier, Root Metric: 10, Metric: 0
  Not eligible, Reason: Primary next-hop link fate sharing
  track-item: glacier.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops
  track-item: glacier.00-00
  track-item: kobuk.00-00
  Not eligible, Reason: Path loops

3 nodes
show isis context-identifier

Syntax

show isis context-identifier
<brief | detail | extensive>
<identifier name>
<instance instance-name>
logical-system (all | logical-system-name)>

Release Information

Command introduced in Junos OS Release 10.4.

Description

Display IS-IS context identifier information.

Options

brief | detail | extensive—(Optional) Display the specified level of output.
identifier name—(Optional) Display information about the specified context identifier.
instance instance-name—(Optional) Display entries for the specified routing instance.
logical-system (all | logical-system-name)—(Optional) Display the context identifier information for all logical systems or for a particular logical system.

Required Privilege

View

Output Fields

Table 130 on page 2069 lists the output fields for the show isis context-identifier command. Output fields are listed in the approximate order in which they appear.

Table 130: show isis context-identifier Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>IPv4 address that defines a protection pair. The context is manually configured on both primary and protector PEs.</td>
<td>detail</td>
</tr>
<tr>
<td>Owner</td>
<td>Protocol that requires the context.</td>
<td>detail</td>
</tr>
<tr>
<td>Role</td>
<td>Role of the PE, which is either primary or protector.</td>
<td>detail</td>
</tr>
<tr>
<td>Primary</td>
<td>Name of the primary PE.</td>
<td>detail</td>
</tr>
<tr>
<td>Metric</td>
<td>Advertised interior gateway protocol (IGP) metric.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

user@host> show isis context-identifier detail

IS-IS context database:
Context    Owner    Role    Primary    Metric

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>2.2.4.3</th>
<th>MPLS</th>
<th>Primary</th>
<th>pro3-e</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertiser pro3-e, Router ID 10.255.245.198, Metric 1, Level 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertiser pro3-e, Router ID 10.255.245.198, Metric 1, Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertiser pro3-c, Router ID 10.255.245.196, Metric 11, Level 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show isis database

**List of Syntax**
Syntax on page 2071
Syntax (EX Series Switches and QFX Series) on page 2071

**Syntax**
show isis database
<system-id>
<brief | detail | extensive>
<instance instance-name>
<level (1 | 2)>
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches and QFX Series)**
show isis database
<system-id>
<brief | detail | extensive>
<level (1 | 2)>
<instance instance-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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Command introduced in Junos OS Release 15.1X53-D30 for the QFX10002 switch.

**Description**
Display the entries in the Intermediate System-to-Intermediate System (IS-IS) link-state database, which contains data about PDU packets.

**Options**
none—Display standard information about IS-IS link-state database entries for all routing instances.

system id—(Optional) Display IS-IS link-state database entries for the specified intermediate system.

brief | detail | extensive—(Optional) Display the specified level of output.

instance instance-name—(Optional) Display IS-IS link-state database entries for the specified routing instance.

level (1 | 2)—(Optional) Display IS-IS link-state database entries for the specified IS-IS level.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view
Related Documentation

- clear isis database on page 2048

List of Sample Output

- show isis database on page 2073
- show isis database brief on page 2074
- show isis database detail on page 2074
- show isis database extensive on page 2075

Output Fields

Table 131 on page 2072 describes the output fields for the show isis database command. Output fields are listed in the approximate order in which they appear. Fields that contain internal IS-IS information useful only in troubleshooting obscure problems are not described in the table. For more details about these fields, contact your customer support representative.

Table 131: show isis database Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Name of the interface on which the link-state PDU has been received; always IS-IS for this command.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
| level | Level of intermediate system:  
- 1—Intermediate system routes within an area; when the destination is outside an area, it routes toward a Level 2 system.  
- 2—Intermediate system routes between areas and toward other ASs. | All levels |
| LSP ID | Link-state PDU identifier. | All levels |
| Sequence | Sequence number of the link-state PDU. | All levels |
| Checksum | Checksum value of the link-state PDU. | All levels |
| Lifetime (secs) | Remaining lifetime of the link-state PDU, in seconds. | All levels |
| Attributes | Attributes of the specified database: L1, L2, Overload, or Attached (L1 only). | none brief |
| # LSPs | Total number of link-state PDUs in the specified link-state database. | none brief |
| IP prefix | Prefix advertised by this link-state PDU. | detail extensive |
| IS neighbor | IS-IS neighbor of the advertising system. | detail extensive |
| IP prefix | IPv4 prefix advertised by this link-state PDU. | detail extensive |
| V6 prefix | IPv6 prefix advertised by this link-state PDU. | detail extensive |
| Metric | Metric of the prefix or neighbor. | detail extensive |
Table 131: show isis database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• LSPID—Link state PDU identifier of the header.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Length—Header length.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Allocated Length—Amount of length available for the header.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• RouterID—Address of the local routing device.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Remaining Lifetime—Remaining lifetime of the link-state PDU, in seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Packet</td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• LSP ID—The identifier for the link-state PDU.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Length—Packet length.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Lifetime—Remaining lifetime, in seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Checksum—The checksum of the link-state PDU.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Sequence—The sequence number of the link-state PDU. Every time the link-state PDU is updated, this number increments.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Attributes—Packet attributes.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• NLPID—Network layer protocol identifier.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Fixed length—Specifies the set length for the packet.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

TLVs

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Area Address—Area addresses that the routing device can reach.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Speaks—Supported routing protocols.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IP routerid—ID of the routing device (usually the IP address).</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IP address—IPv4 address.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Hostname—Assigned name of the routing device.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IP prefix—IP prefix of the routing device.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Metric—IS-IS metric that measures the cost of the adjacency between the originating routing device and the advertised routing device.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IP extended prefix—Extended IP prefix of the routing device.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IS neighbor—Directly attached neighbor’s name and metric.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• IS extended neighbor—Directly attached neighbor’s name, metric, IP address, local interface index, and remote interface index.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• The interface indexes enable Junos OS to support unnumbered extensions for IS-IS, as described in RFC 4205.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Router Capability—ID of the routing device and flag.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Note: Router capability also specifies SPRING capability and SPRING algorithm when segment routing is enabled on the routing device.

Sample Output

tableau@host> show isis database

    IS-IS level 1 link-state database:
    LSP ID | Sequence | Checksum | Lifetime | Attributes |
    --- | --- | --- | --- | --- |
    kobuk.00-00 | 0x3 | 0x3167 | 1057 | L1 L2 |
    camaro.00-00 | 0x5 | 0x770e | 1091 | L1 L2 |
    ranier.00-00 | 0x4 | 0xaa95 | 1091 | L1 L2 |
    glacier.00-00 | 0x4 | 0x206f | 1089 | L1 L2 |
    glacier.02-00 | 0x1 | 0xd141 | 1089 | L1 L2 |
show isis database brief

The output for the show isis database brief command is identical to that for the show isis database command. For sample output, see show isis database on page 2073.

show isis database detail

user@host> show isis database logical-system CE3 sisira.00-00 detail

IS-IS level 1 link-state database:

sisira.00-00 Sequence: 0x11, Checksum: 0x10fc, Lifetime: 975 secs
IS neighbor: hemantha-CE3.02 Metric: 10
ES neighbor: 0015.0015.0015 Metric: 10 Down
ES neighbor: 0025.0025.0025 Metric: 10 Down
ES neighbor: 0030.0030.0030 Metric: 10 Down
ES neighbor: 0040.0040.0040 Metric: 10 Down
ES neighbor: sisira Metric: 0
IP prefix: 1.0.0.0/24 Metric: 10 External Down
IP prefix: 3.0.0.0/24 Metric: 10 External Down
IP prefix: 4.0.0.0/24 Metric: 10 External Down
IP prefix: 5.0.0.0/24 Metric: 10 External Up
IP prefix: 15.15.15.15/32 Metric: 10 External Down
IP prefix: 25.25.25.25/32 Metric: 10 External Down
IP prefix: 30.30.30.30/32 Metric: 10 External Down
IP prefix: 40.40.40.40/32 Metric: 10 External Down
IP prefix: 60.60.60.60/32 Metric: 0 Internal Up

IS-IS level 2 link-state database:

sisira.00-00 Sequence: 0x13, Checksum: 0x69ac, Lifetime: 993 secs
IS neighbor: hemantha-CE3.02 Metric: 10
IP prefix: 1.0.0.0/24 Metric: 10 External Down
IP prefix: 3.0.0.0/24 Metric: 10 External Down
IP prefix: 4.0.0.0/24 Metric: 10 External Down
IP prefix: 5.0.0.0/24 Metric: 10 Internal Up
IP prefix: 15.15.15.15/32 Metric: 10 External Down
IP prefix: 25.25.25.25/32 Metric: 10 External Down
IP prefix: 30.30.30.30/32 Metric: 10 External Down
IP prefix: 40.40.40.40/32 Metric: 10 External Down
IP prefix: 50.50.50.50/32 Metric: 10 Internal Up
IP prefix: 60.60.60.60/32 Metric: 0 Internal Up
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0015.0015.0015/152 Metric: 10 External Down
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0025.0025.0025/152 Metric: 10 External Down
show isis database extensive

user@host> show isis database extensive

IS-IS level 1 link-state database:

sisira.00-00 Sequence: 0x11, Checksum: 0x10fc, Lifetime: 970 secs
IS neighbor: hemantha-CE3.02   Metric:       10
Two-way fragment: hemantha-CE3.02-00, Two-way first fragment:

hemantha-CE3.02-00
ES neighbor: 0015.0015.0015   Metric:       10 Down
ES neighbor: 0025.0025.0025   Metric:       10 Down
ES neighbor: 0030.0030.0030   Metric:       10 Down
ES neighbor: 0040.0040.0040   Metric:       10 Down
ES neighbor: sisira           Metric:       0
IP prefix: 1.0.0.0/24         Metric:       10 External Down
IP prefix: 3.0.0.0/24         Metric:       10 External Down
IP prefix: 4.0.0.0/24         Metric:       10 External Down
IP prefix: 5.0.0.0/24         Metric:       10 Internal Up
IP prefix: 15.15.15.15/32     Metric:       10 External Down
IP prefix: 25.25.25.25/32     Metric:       10 External Down
IP prefix: 30.30.30.30/32     Metric:       10 External Down
IP prefix: 40.40.40.40/32     Metric:       10 External Down
IP prefix: 60.60.60.60/32     Metric:       0 Internal Up

Header: LSP ID: sisira.00-00, Length: 336 bytes
Allocated length: 336 bytes, Router ID: 0.0.0.0
Remaining lifetime: 970 secs, Level: 1, Interface: 333
Estimated free bytes: 144, Actual free bytes: 0
Aging timer expires in: 970 secs
Protocols: IP, IPv6, CLNS

Packet: LSP ID: sisira.00-00, Length: 336 bytes, Lifetime : 1198 secs
Checksum: 0x10fc, Sequence: 0x11, Attributes: 0x83 L1 L2 Attached
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 18, Packet version: 1, Max area: 0

TLVs:
Area address: 60.0006.80ff.f800.0000.0108.0001 (13)
Speaks: IP
Speaks: IPv6
Speaks: CLNP
Hostname: sisira
ES neighbor TLV: Internal, Metric: default 0, Up
ES: sisira
IS neighbor: hemantha-CE3.02, Internal, Metric: default 10
IS extended neighbor: hemantha-CE3.02, Metric: default 10
ES neighbor TLV: External, Metric: default 10, Down
ES: 0040.0040.0040
ES neighbor TLV: External, Metric: default 10, Down
ES: 0025.0025.0025
ES neighbor TLV: External, Metric: default 10, Down
ES: 0015.0015.0015
ES neighbor TLV: External, Metric: default 10, Down
ES: 0030.0030.0030
IP external prefix: 3.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 4.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 25.25.25.25/32, Internal, Metric: default 10, Down
IP external prefix: 15.15.15.15/32, Internal, Metric: default 10, Down
IP external prefix: 1.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 30.30.30.30/32, Internal, Metric: default 10, Down
IP extended prefix: 3.0.0.0/24 metric 10 down
IP extended prefix: 4.0.0.0/24 metric 10 down
IP extended prefix: 25.25.25.25/32 metric 10 down
IP extended prefix: 15.15.15.15/32 metric 10 down
IP extended prefix: 1.0.0.0/24 metric 10 down
IP extended prefix: 30.30.30.30/32 metric 10 down
IP prefix: 60.60.60.60/32, Internal, Metric: default 0, Up
IP prefix: 5.0.0.0/24, Internal, Metric: default 10, Up
IP extended prefix: 60.60.60.60/32 metric 0 up
IP extended prefix: 5.0.0.0/24 metric 10 up
No queued transmissions

IS-IS level 2 link-state database:

Router-A.00-00 Sequence: 0x5, Checksum: 0x3196, Lifetime: 1158 secs
    IS neighbor: Router-B.02 Metric: 10
        Two-way fragment: Router-B.02-00, Two-way first fragment: Router-B.02-00
    IS neighbor: Router-E.02 Metric: 10
        Two-way fragment: Router-E.02-00, Two-way first fragment: Router-E.02-00
    IP prefix: 10.0.0.0/30 Metric: 10 Internal Up
    IP prefix: 10.0.0.4/30 Metric: 10 Internal Up
    IP prefix: 192.168.0.1/32 Metric: 0 Internal Up

Header: LSP ID: Router-A.00-00, Length: 208 bytes
    Allocated length: 1492 bytes, Router ID: 192.168.0.1
    Remaining lifetime: 1158 secs, Level: 2, Interface: 0
    Estimated free bytes: 1233, Actual free bytes: 1284
    Aging timer expires in: 1158 secs
    Protocols: IP, IPv6

Packet: LSP ID: Router-A.00-00, Length: 208 bytes, Lifetime: 1198 secs
    Checksum: 0x3196, Sequence: 0x5, Attributes: 0x3 <L1 L2>
    NLPIID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
    Packet type: 20, Packet version: 1, Max area: 0

TLVs:
    Area address: 49.0002 (3)
    LSP Buffer Size: 1492
    Speaks: IP
    Speaks: IPv6
    IP router id: 192.168.0.1
    IP address: 192.168.0.1
    Hostname: Router-A
    IP prefix: 192.168.0.1/32, Internal, Metric: default 0, Up
    IP prefix: 10.0.0.4/30, Internal, Metric: default 10, Up
    IP prefix: 10.0.0.0/30, Internal, Metric: default 10, Up
    IP extended prefix: 192.168.0.1/32 metric 0 up
    IP extended prefix: 10.0.0.4/30 metric 10 up
IP extended prefix: 10.0.0.0/30 metric 10 up
IS neighbor: Router-E.02, Internal, Metric: default 10
IS neighbor: Router-B.02, Internal, Metric: default 10
IS extended neighbor: Router-E.02, Metric: default 10
  IP address: 10.0.0.1
    Local interface index: 101, Remote interface index: 0
IS extended neighbor: Router-B.02, Metric: default 10
  IP address: 10.0.0.5
    Local interface index: 102, Remote interface index: 0
No queued transmissions

Router-B.00-00 Sequence: 0x5, Checksum: 0xf8f, Lifetime: 1183 secs
  IS neighbor: Router-B.02
    Metric: 10
  Two-way fragment: Router-B.02-00, Two-way first fragment: Router-B.02-00
  IS neighbor: Router-C.02
    Metric: 10
  Two-way fragment: Router-C.02-00, Two-way first fragment: Router-C.02-00
  IP prefix: 10.0.0.4/30
    Metric: 10 Internal Up
  IP prefix: 10.0.0.8/30
    Metric: 10 Internal Up
  IP prefix: 192.168.0.2/32
    Metric: 0 Internal Up

Header: LSP ID: Router-B.00-00, Length: 208 bytes
  Allocated length: 284 bytes, Router ID: 192.168.0.2
  Remaining lifetime: 1183 secs, Level: 2, Interface: 102
  Estimated free bytes: 114, Actual free bytes: 76
  Aging timer expires in: 1183 secs
  Protocols: IP, IPv6

Packet: LSP ID: Router-B.00-00, Length: 208 bytes, Lifetime : 1196 secs
  Checksum: 0xf8f, Sequence: 0x5, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  Area address: 49.0002 (3)
  LSP Buffer Size: 1492
  Speaks: IP
  Speaks: IPv6
  IP router id: 192.168.0.2
  IP address: 192.168.0.2
  Hostname: Router-B
  IP prefix: 192.168.0.2/32, Internal, Metric: default 0, Up
  IP prefix: 10.0.0.4/30, Internal, Metric: default 10, Up
  IP prefix: 10.0.0.8/30, Internal, Metric: default 10, Up
  IP extended prefix: 192.168.0.2/32 metric 0 up
  IP extended prefix: 10.0.0.4/30 metric 10 up
  IP extended prefix: 10.0.0.8/30 metric 10 up
  IS neighbor: Router-B.02, Internal, Metric: default 10
  IS neighbor: Router-C.02, Internal, Metric: default 10
  IS extended neighbor: Router-B.02, Metric: default 10
    IP address: 10.0.0.6
      Local interface index: 108, Remote interface index: 0
    IS extended neighbor: Router-C.02, Metric: default 10
      IP address: 10.0.0.9
        Local interface index: 109, Remote interface index: 0
No queued transmissions

Router-B.02-00 Sequence: 0x1, Checksum: 0x3c7c, Lifetime: 1156 secs
  IS neighbor: Router-A.00
    Metric: 0
  Two-way fragment: Router-A.00-00, Two-way first fragment: Router-A.00-00
  IS neighbor: Router-B.00
    Metric: 0
Two-way fragment: Router-B.00-00, Two-way first fragment: Router-B.00-00

Header: LSP ID: Router-B.02-00, Length: 76 bytes
Allocated length: 284 bytes, Router ID: 0.0.0.0
Remaining lifetime: 1156 secs, Level: 2, Interface: 102
Estimated free bytes: 208, Actual free bytes: 208
Aging timer expires in: 1156 secs

Packet: LSP ID: Router-B.02-00, Length: 76 bytes, Lifetime : 1196 secs
Checksum: 0x3c7c, Sequence: 0x1, Attributes: 0x3 <L1 L2>
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
IS neighbor: Router-B.00, Internal, Metric: default 0
IS neighbor: Router-A.00, Internal, Metric: default 0
IS extended neighbor: Router-B.00, Metric: default 0
IS extended neighbor: Router-A.00, Metric: default 0
No queued transmissions

Router-C.00-00 Sequence: 0x5, Checksum: 0x255b, Lifetime: 1182 secs
Two-way fragment: Router-C.02-00, Two-way first fragment: Router-C.02-00
Two-way fragment: Router-D.03-00, Two-way first fragment: Router-D.03-00
IP prefix: 10.0.0.8/30, Metric: default 10 Internal Up
IP prefix: 10.0.0.12/30, Metric: default 10 Internal Up
IP prefix: 192.168.0.3/32, Metric: default 0 Up

Header: LSP ID: Router-C.00-00, Length: 208 bytes
Allocated length: 284 bytes, Router ID: 192.168.0.3
Remaining lifetime: 1182 secs, Level: 2, Interface: 102
Estimated free bytes: 114, Actual free bytes: 76
Aging timer expires in: 1182 secs
Protocols: IP, IPv6

Packet: LSP ID: Router-C.00-00, Length: 208 bytes, Lifetime : 1196 secs
Checksum: 0x255b, Sequence: 0x5, Attributes: 0x3 <L1 L2>
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
Area address: 49.0002 (3)
LSP Buffer Size: 1492
Speaks: IP
Speaks: IPv6
IP router id: 192.168.0.3
IP address: 192.168.0.3
Hostname: Router-C
IP prefix: 192.168.0.3/32, Internal, Metric: default 0, Up
IP prefix: 10.0.0.8/30, Internal, Metric: default 10, Up
IP prefix: 10.0.0.12/30, Internal, Metric: default 10, Up
IP extended prefix: 192.168.0.3/32 metric 0 up
IP extended prefix: 10.0.0.8/30 metric 10 up
IP extended prefix: 10.0.0.12/30 metric 10 up
IS neighbor: Router-C.02, Internal, Metric: default 10
IS neighbor: Router-D.03, Internal, Metric: default 10
IS extended neighbor: Router-C.02, Metric: default 10
IP address: 10.0.0.10
Local interface index: 105, Remote interface index: 0
IS extended neighbor: Router-D.03, Metric: default 10
  IP address: 10.0.0.13
  Local interface index: 106, Remote interface index: 0
  No queued transmissions

Router-C.02-00 Sequence: 0x1, Checksum: 0xaaa09, Lifetime: 1181 secs
  IS neighbor: Router-B.00, Metric: 0
  Two-way fragment: Router-B.00-00, Two-way first fragment: Router-B.00-00
  IS neighbor: Router-C.00, Metric: 0
  Two-way fragment: Router-C.00-00, Two-way first fragment: Router-C.00-00

Header: LSP ID: Router-C.02-00, Length: 76 bytes
  Allocated length: 284 bytes, Router ID: 0.0.0.0
  Remaining lifetime: 1181 secs, Level: 2, Interface: 102
  Estimated free bytes: 208, Actual free bytes: 208
  Aging timer expires in: 1181 secs

Packet: LSP ID: Router-C.02-00, Length: 76 bytes, Lifetime: 1194 secs
  Checksum: 0xaaa09, Sequence: 0x1, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  IS neighbor: Router-C.00, Internal, Metric: default 0
  IS neighbor: Router-B.00, Internal, Metric: default 0
  IS extended neighbor: Router-C.00, Metric: default 0
  IS extended neighbor: Router-B.00, Metric: default 0
  No queued transmissions

Router-D.00-00 Sequence: 0x4, Checksum: 0x8ab7, Lifetime: 1180 secs
  IS neighbor: Router-D.02, Metric: 10
  Two-way fragment: Router-D.02-00, Two-way first fragment: Router-D.02-00
  IS neighbor: Router-D.03, Metric: 10
  Two-way fragment: Router-D.03-00, Two-way first fragment: Router-D.03-00
  IP prefix: 10.0.0.12/30, Metric: default 10, Up
  IP prefix: 10.0.0.20/30, Metric: default 10, Up
  IP prefix: 192.168.0.4/32, Metric: default 0, Up

Header: LSP ID: Router-D.00-00, Length: 208 bytes
  Allocated length: 284 bytes, Router ID: 192.168.0.4
  Remaining lifetime: 1180 secs, Level: 2, Interface: 102
  Estimated free bytes: 114, Actual free bytes: 76
  Aging timer expires in: 1180 secs
  Protocols: IP, IPv6

Packet: LSP ID: Router-D.00-00, Length: 208 bytes, Lifetime: 1192 secs
  Checksum: 0x8ab7, Sequence: 0x4, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  Area address: 49.0002 (3)
  LSP Buffer Size: 1492
  Speaks: IP
  Speaks: IPv6
  IP router id: 192.168.0.4
  IP address: 192.168.0.4
  Hostname: Router-D
  IP prefix: 192.168.0.4/32, Internal, Metric: default 0, Up
  IP prefix: 10.0.0.12/30, Internal, Metric: default 10, Up
IP prefix: 10.0.0.20/30, Internal, Metric: default 10, Up
IP extended prefix: 192.168.0.4/32 metric 0 up
IP extended prefix: 10.0.0.12/30 metric 10 up
IP extended prefix: 10.0.0.20/30 metric 10 up
IS neighbor: Router-D.02, Internal, Metric: default 10
IS neighbor: Router-D.03, Internal, Metric: default 10
IS extended neighbor: Router-D.02, Metric: default 10
IP address: 10.0.0.22
  Local interface index: 115, Remote interface index: 0
IS extended neighbor: Router-D.03, Metric: default 10
IP address: 10.0.0.14
  Local interface index: 114, Remote interface index: 0
No queued transmissions

Router-D.02-00 Sequence: 0x1, Checksum: 0xebb0, Lifetime: 1128 secs
  IS neighbor: Router-D.00, Metric: 0
    Two-way fragment: Router-D.00-00, Two-way first fragment: Router-D.00-00
  IS neighbor: Router-F.00, Metric: 0
    Two-way fragment: Router-F.00-00, Two-way first fragment: Router-F.00-00

Header: LSP ID: Router-D.02-00, Length: 76 bytes
  Allocated length: 284 bytes, Router ID: 0.0.0.0
  Remaining lifetime: 1128 secs, Level: 2, Interface: 101
  Estimated free bytes: 208, Actual free bytes: 208
  Aging timer expires in: 1128 secs
Packet: LSP ID: Router-D.02-00, Length: 76 bytes, Lifetime: 1160 secs
  Checksum: 0xebb0, Sequence: 0x1, Attributes: 0x3 <l1 l2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0
TLVs:
  IS neighbor: Router-D.00, Internal, Metric: default 0
  IS neighbor: Router-F.00, Internal, Metric: default 0
  IS extended neighbor: Router-D.00, Metric: default 0
  IS extended neighbor: Router-F.00, Metric: default 0
No queued transmissions

Router-D.03-00 Sequence: 0x1, Checksum: 0x129b, Lifetime: 1180 secs
  IS neighbor: Router-C.00, Metric: 0
    Two-way fragment: Router-C.00-00, Two-way first fragment: Router-C.00-00
  IS neighbor: Router-D.00, Metric: 0
    Two-way fragment: Router-D.00-00, Two-way first fragment: Router-D.00-00

Header: LSP ID: Router-D.03-00, Length: 76 bytes
  Allocated length: 284 bytes, Router ID: 0.0.0.0
  Remaining lifetime: 1180 secs, Level: 2, Interface: 101
  Estimated free bytes: 208, Actual free bytes: 208
  Aging timer expires in: 1180 secs
Packet: LSP ID: Router-D.03-00, Length: 76 bytes, Lifetime: 1192 secs
  Checksum: 0x129b, Sequence: 0x1, Attributes: 0x3 <l1 l2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0
TLVs:
  IS neighbor: Router-D.00, Internal, Metric: default 0
  IS neighbor: Router-C.00, Internal, Metric: default 0
  IS extended neighbor: Router-D.00, Metric: default 0
  IS extended neighbor: Router-C.00, Metric: default 0
No queued transmissions

Router-E.00-00 Sequence: 0x4, Checksum: 0x9da9, Lifetime: 1155 secs
IS neighbor: Router-E.02  Metric: 10
  Two-way fragment: Router-E.02-00, Two-way first fragment: Router-E.02-00
IS neighbor: Router-F.02  Metric: 20
  Two-way fragment: Router-F.02-00, Two-way first fragment: Router-F.02-00
IP prefix: 10.0.0.0/30  Metric: 10 Internal Up
IP prefix: 10.0.0.16/30  Metric: 20 Internal Up
IP prefix: 192.168.0.5/32  Metric: 0 Internal Up

Header: LSP ID: Router-E.00-00, Length: 208 bytes
  Allocated length: 284 bytes, Router ID: 192.168.0.5
  Remaining lifetime: 1155 secs, Level: 2, Interface: 101
  Estimated free bytes: 114, Actual free bytes: 76
  Aging timer expires in: 1155 secs
  Protocols: IP, IPv6

Packet: LSP ID: Router-E.00-00, Length: 208 bytes, Lifetime : 1185 secs
  Checksum: 0x9da9, Sequence: 0x4, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  Area address: 49.0002 (3)
  LSP Buffer Size: 1492
  Speaks: IP
  Speaks: IPV6
  IP router id: 192.168.0.5
  IP address: 192.168.0.5
  Hostname: Router-E
  IP prefix: 192.168.0.5/32, Internal, Metric: default 0, Up
  IP prefix: 10.0.0.16/30, Internal, Metric: default 20, Up
  IP prefix: 10.0.0.0/30, Internal, Metric: default 10, Up
  IP extended prefix: 192.168.0.5/32 metric 0 up
  IP extended prefix: 10.0.0.16/30 metric 20 up
  IP extended prefix: 10.0.0.0/30 metric 10 up
  IS neighbor: Router-E.02, Internal, Metric: default 10
  IS neighbor: Router-F.02, Internal, Metric: default 20
  IS extended neighbor: Router-E.02, Metric: default 10
  IP address: 10.0.0.2
    Local interface index: 112, Remote interface index: 0
  IS extended neighbor: Router-F.02, Metric: default 20
    IP address: 10.0.0.17
    Local interface index: 111, Remote interface index: 0
No queued transmissions

Router-E.02-00 Sequence: 0x1, Checksum: 0xb4fa, Lifetime: 1130 secs
IS neighbor: Router-A.00  Metric: 0
  Two-way fragment: Router-A.00-00, Two-way first fragment: Router-A.00-00
IS neighbor: Router-E.00  Metric: 0
  Two-way fragment: Router-E.00-00, Two-way first fragment: Router-E.00-00

Header: LSP ID: Router-E.02-00, Length: 76 bytes
  Allocated length: 284 bytes, Router ID: 0.0.0.0
  Remaining lifetime: 1130 secs, Level: 2, Interface: 101
  Estimated free bytes: 208, Actual free bytes: 208
  Aging timer expires in: 1130 secs

Packet: LSP ID: Router-E.02-00, Length: 76 bytes, Lifetime : 1161 secs
Checksum: 0xb4fa, Sequence: 0x1, Attributes: 0x3 <L1 L2>
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  IS neighbor: Router-E.00, Internal, Metric: default 0
  IS neighbor: Router-A.00, Internal, Metric: default 0
  IS extended neighbor: Router-E.00, Metric: default 0
  IS extended neighbor: Router-A.00, Metric: default 0

No queued transmissions

Router-F.00-00 Sequence: 0x5, Checksum: 0x94bd, Lifetime: 1153 secs
  IS neighbor: Router-D.02                      Metric:       10
  Two-way fragment: Router-D.02-00, Two-way first fragment: Router-D.02-00
  IS neighbor: Router-F.02                      Metric:       10
  Two-way fragment: Router-F.02-00, Two-way first fragment: Router-F.02-00
  IP prefix: 10.0.0.16/30                    Metric:       10 Internal Up
  IP prefix: 10.0.0.20/30                    Metric:       10 Internal Up
  IP prefix: 192.168.0.6/32                  Metric:        0 Internal Up

Header: LSP ID: Router-F.00-00, Length: 208 bytes
  Allocated length: 284 bytes, Router ID: 192.168.0.6
  Remaining lifetime: 1153 secs, Level: 2, Interface: 101
  Estimated free bytes: 76, Actual free bytes: 76
  Aging timer expires in: 1153 secs
  Protocols: IP, IPv6

Packet: LSP ID: Router-F.00-00, Length: 208 bytes, Lifetime: 1183 secs
  Checksum: 0x94bd, Sequence: 0x5, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  Area address: 49.0002 (3)
  LSP Buffer Size: 1492
  Speaks: IP
  Speaks: IPv6
  IP router id: 192.168.0.6
  IP address: 192.168.0.6
  Hostname: Router-F
  IP prefix: 192.168.0.6/32, Internal, Metric: default 0, Up
  IP prefix: 10.0.0.16/30, Internal, Metric: default 10, Up
  IP prefix: 10.0.0.20/30, Internal, Metric: default 10, Up
  IP extended prefix: 192.168.0.6/32 metric 0 up
  IP extended prefix: 10.0.0.16/30 metric 10 up
  IP extended prefix: 10.0.0.20/30 metric 10 up
  IS neighbor: Router-D.02, Internal, Metric: default 10
  IS neighbor: Router-F.02, Internal, Metric: default 10
  IS extended neighbor: Router-D.02, Metric: default 10
  IP address: 10.0.0.21
  Local interface index: 94, Remote interface index: 0
  IS extended neighbor: Router-F.02, Metric: default 10
  IP address: 10.0.0.18
  Local interface index: 93, Remote interface index: 0

No queued transmissions

Router-E.02-00 Sequence: 0x1, Checksum: 0xb4fa, Lifetime: 1130 secs
  IS neighbor: Router-A.00                      Metric:        0
  Two-way fragment: Router-A.00-00, Two-way first fragment: Router-A.00-00
  IS neighbor: Router-E.00                      Metric:        0
Two-way fragment: Router-E.00-00, Two-way first fragment: Router-E.00-00

Header: LSP ID: Router-E.02-00, Length: 76 bytes
Allocated length: 284 bytes, Router ID: 0.0.0.0
Remaining lifetime: 1130 secs, Level: 2, Interface: 101
Estimated free bytes: 208, Actual free bytes: 208
Aging timer expires in: 1130 secs

Packet: LSP ID: Router-E.02-00, Length: 76 bytes, Lifetime : 1161 secs
Checksum: 0xb4fa, Sequence: 0x1, Attributes: 0x3 <L1 L2>
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
IS neighbor: Router-E.00, Internal, Metric: default 0
IS neighbor: Router-A.00, Internal, Metric: default 0
IS extended neighbor: Router-E.00, Metric: default 0
IS extended neighbor: Router-A.00, Metric: default 0
No queued transmissions

Router-F.00-00 Sequence: 0x5, Checksum: 0x94bd, Lifetime: 1153 secs
IS neighbor: Router-D.02, Metric: 10
Two-way fragment: Router-D.02-00, Two-way first fragment: Router-D.02-00
IS neighbor: Router-F.02, Metric: 10
Two-way fragment: Router-F.02-00, Two-way first fragment: Router-F.02-00
IP prefix: 10.0.0.16/30 Metric: 10 Internal Up
IP prefix: 10.0.0.20/30 Metric: 10 Internal Up
IP prefix: 192.168.0.6/32 Metric: 0 Internal Up

Header: LSP ID: Router-F.00-00, Length: 208 bytes
Allocated length: 284 bytes, Router ID: 192.168.0.6
Remaining lifetime: 1153 secs, Level: 2, Interface: 101
Estimated free bytes: 76, Actual free bytes: 76
Aging timer expires in: 1153 secs
Protocols: IP, IPv6

Packet: LSP ID: Router-F.00-00, Length: 208 bytes, Lifetime : 1183 secs
Checksum: 0x94bd, Sequence: 0x5, Attributes: 0x3 <L1 L2>
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
Area address: 49.0002 (3)
LSP Buffer Size: 1492
Speaks: IP
Speaks: IPv6
IP router id: 192.168.0.6
IP address: 192.168.0.6
Hostname: Router-F
IP prefix: 192.168.0.6/32, Internal, Metric: default 0, Up
IP prefix: 10.0.0.16/30, Internal, Metric: default 10, Up
IP prefix: 10.0.0.20/30, Internal, Metric: default 10, Up
IP extended prefix: 192.168.0.6/32 metric 0 up
IP extended prefix: 10.0.0.16/30 metric 10 up
IP extended prefix: 10.0.0.20/30 metric 10 up
IS neighbor: Router-D.02, Internal, Metric: default 10
IS neighbor: Router-F.02, Internal, Metric: default 10
IS extended neighbor: Router-D.02, Metric: default 10
IS extended neighbor: Router-F.02, Metric: default 10
IP address: 10.0.0.21
Local interface index: 94, Remote interface index: 0
IS extended neighbor: Router-F.02, Metric: default 10
  IP address: 10.0.0.18
  Local interface index: 93, Remote interface index: 0
  No queued transmissions

Router-F.02-00 Sequence: 0x1, Checksum: 0xf5ae, Lifetime: 1153 secs
  IS neighbor: Router-E.00                      Metric:        0
    Two-way fragment: Router-E.00-00, Two-way first fragment: Router-E.00-00
  IS neighbor: Router-F.00                      Metric:        0
    Two-way fragment: Router-F.00-00, Two-way first fragment: Router-F.00-00

Header: LSP ID: Router-F.02-00, Length: 76 bytes
  Allocated length: 284 bytes, Router ID: 0.0.0.0
  Remaining lifetime: 1153 secs, Level: 2, Interface: 101
  Estimated free bytes: 208, Actual free bytes: 208
  Aging timer expires in: 1153 secs

Packet: LSP ID: Router-F.02-00, Length: 76 bytes, Lifetime: 1183 secs
  Checksum: 0xf5ae, Sequence: 0x1, Attributes: 0x3 <L1 L2>
  NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
  Packet type: 20, Packet version: 1, Max area: 0

TLVs:
  IS neighbor: Router-F.00, Internal, Metric: default 0
  IS neighbor: Router-E.00, Internal, Metric: default 0
  IS extended neighbor: Router-F.00, Metric: default 0
  IS extended neighbor: Router-E.00, Metric: default 0
  No queued transmissions
show isis hostname

**List of Syntax**

Syntax on page 2085
Syntax (EX Series Switches and QFX Series) on page 2085

**Syntax**

show isis hostname

<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches and QFX Series)**

show isis hostname

**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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display IS-IS hostname database information.

This command displays the system ID-to-name cache. The output shows if the mapping has been learned by receipt of a Hostname TLV #137 (type dynamic) configured in Junos OS with the set system host-name command, or a static mapping defined in Junos OS with the set system static-host-mapping hostname sysid command (type static). The local router always has its type set to static even if static-host-mapping is not configured.

**Options**

none—Display IS-IS hostname database information.

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 isis hostname on page 2086

**Output Fields**

Table 132 on page 2085 describes the output fields for the show isis hostname command. Output fields are listed in the approximate order in which they appear.

**Table 132: show isis hostname Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>System identifier mapped to the hostname.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname mapped to the system identifier.</td>
</tr>
</tbody>
</table>
### Table 132: show isis hostname Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Type of mapping between system identifier and hostname.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic</strong>—Hostname mapping determined as described in RFC 2763, <em>Dynamic Hostname Exchange Mechanism for IS-IS</em>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Static</strong>—Hostname mapping configured by user.</td>
</tr>
</tbody>
</table>

---

**Sample Output**

```
show isis hostname
```

```
user@host> show isis hostname
IS-IS hostname database:
  System Id  Hostname        Type
  1921.6800.4201 isis1       Dynamic
  1921.6800.4202 isis2       Static
  1921.6800.4203 isis3       Dynamic
```
### show isis interface

#### List of Syntax
- Syntax: Syntax on page 2087
  - Syntax (EX Series Switches and QFX Series) on page 2087

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show isis interface &lt;brief</td>
<td>detail</td>
</tr>
</tbody>
</table>

#### Syntax (EX Series Switches and QFX Series)
- show isis interface <brief | detail | extensive> <interface-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 12.1 for the QFX Series.

#### Description

**NOTE:** If the configured metric for an IS-IS level is above 63, and the wide-metrics-only statement is not configured, the show isis interface detail command and the show isis interface extensive command display 63 as the metric value for that level. Configure the wide-metrics-only statement to generate metric values greater than 63 on a per IS-IS level basis.

The show isis interface command displays the configured metric value for an IS-IS level irrespective of whether is configured or not.

#### Options
- **none**—Display standard information about all IS-IS-enabled interfaces.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display information about the specified interface only.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

#### Required Privilege Level
- view

#### Related Documentation
- [Understanding Wide IS-IS Metrics for Traffic Engineering](#)
- [Example: Enabling Wide IS-IS Metrics for Traffic Engineering](#)
List of Sample Output  show isis interface on page 2090  
show isis interface brief on page 2090  
show isis interface detail on page 2090  
show isis interface extensive on page 2090

Output Fields  Table 133 on page 2088 describes the output fields for the show isis interface command. Output fields are listed in the approximate order in which they appear.

Table 133: show isis 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-name</td>
<td>Name of the interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Designated router</td>
<td>Routing device selected by other routers that is responsible for sending link-state advertisements that describe the network. Used only on broadcast networks.</td>
<td>detail</td>
</tr>
<tr>
<td>Index</td>
<td>Interface index assigned by the Junos OS kernel.</td>
<td>detail</td>
</tr>
<tr>
<td>State</td>
<td>Internal implementation information.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit id</td>
<td>Circuit identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit type</td>
<td>Circuit type:</td>
<td>detail</td>
</tr>
<tr>
<td>LSP interval</td>
<td>Interval between link-state PDUs sent from the interface.</td>
<td>detail</td>
</tr>
<tr>
<td>CSNP interval</td>
<td>Interval between complete sequence number PDUs sent from the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Sysid</td>
<td>System identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the adjacency is made.</td>
<td>none brief</td>
</tr>
<tr>
<td>L or Level</td>
<td>Level:</td>
<td>All levels</td>
</tr>
<tr>
<td>CirID</td>
<td>Circuit identifier.</td>
<td>none brief</td>
</tr>
</tbody>
</table>
### Table 133: show isis 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>Level 1 DR</strong></td>
<td>Level 1 designated intermediate system.</td>
<td>none brief</td>
</tr>
<tr>
<td><strong>Level 2 DR</strong></td>
<td>Level 2 designated intermediate system.</td>
<td>none brief</td>
</tr>
<tr>
<td><strong>L1/L2 Metric</strong></td>
<td>Interface’s metric for Level 1 and Level 2. If there is no information, the metric is 0.</td>
<td>none brief</td>
</tr>
<tr>
<td><strong>Flood-group Area-ID</strong></td>
<td>Flood-group is configured on a specific IS-IS interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Adjacency advertisement: Advertise</strong></td>
<td>This routing device has signaled to advertise this interface to its neighbors in their label-switched paths (LSPs).</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Adjacency advertisement: Suppress</strong></td>
<td>This neighbor has signaled not to advertise this interface in the routing device’s outbound LSPs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Adjacencies</strong></td>
<td>Number of adjacencies established on this interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Priority value for this interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Metric value for this interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Hello(s) / Hello Interval</strong></td>
<td>Interface’s hello interval.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Hold(s) / HoldTime</strong></td>
<td>Interface’s hold time.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Designated Router</strong></td>
<td>Router responsible for sending network link-state advertisements, which describe all the routing devices attached to the network.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Hello padding</strong></td>
<td>Type of hello padding:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Adaptive—On point-to-point connections, the hello packets are padded from the initial detection of a new neighbor until the neighbor verifies the adjacency as Up in the adjacency state TLV. If the neighbor does not support the adjacency state TLV, then padding continues. On LAN connections, padding starts from the initial detection of a new neighbor until there is at least one active adjacency on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loose—(Default) The hello packet is padded from the initial detection of a new neighbor until the adjacency transitions to the Up state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strict—Padding is performed on all interface types and for all adjacency states, and is continuous.</td>
<td></td>
</tr>
<tr>
<td><strong>LDP sync state</strong></td>
<td>Current LDP synchronization state: in sync, in holddown, or not supported.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>reason</strong></td>
<td>Reason for being in the LDP sync state.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 133: show isis 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>config holdtime</td>
<td>Configured value of the hold timer.</td>
<td>extensive</td>
</tr>
<tr>
<td>remaining</td>
<td>If the state is not in sync and the hold time is not infinity, then this field displays the remaining hold time in seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>IIH max size</td>
<td>Configured value of IS-IS hello packets</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show isis interface

```
user@host> show isis interface
IS-IS interface database:
   Interface        L CirID Level 1 DR           Level 2 DR        L1/L2 Metric
at-2/3/0.0        3   0x1 Point to Point    Point to Point         10/10
lo0.0             3   0x1 Passive           Passive                 0/0
```

show isis interface brief

The output for the `show isis interface brief` command is identical to that for the `show isis interface` command. For sample output, see `show isis interface on page 2090`.

show isis interface detail

```
user@host> show isis interface detail
IS-IS interface database:
at-2/3/0.0
   Index: 66, State: 0x6, Circuit id: 0x1, Circuit type: 3
   LSP interval: 100 ms, CSNP interval: 5 s
   Level Adjacencies Priority Metric Hello (s) Hold (s) Designated Router
   1             1       64     10     9.000       27
   2             1       64     10     9.000       27
lo0.0
   Index: 64, State: 0x6, Circuit id: 0x1, Circuit type: 0
   LSP interval: 100 ms, CSNP interval: disabled
   Adjacency advertisement: Advertise
   Protection Type: Node Link, No eligible Backup
   Level Adjacencies Priority Metric Hello (s) Hold (s) Designated Router
   1             0       64      0 Passive
   2             0       64      0 Passive
```

show isis interface extensive

```
user@host> show isis interface extensive
IS-IS interface database:
x-6/1/0.0
   Index: 75, State: 0x6, Circuit id: 0x1, Circuit type: 2
   LSP interval: 100 ms, CSNP interval: 10 s, Loose Hello padding, IIH max size: 1505
```
Adjacency advertisement: Advertise
Flood-group Area-ID: 49.0001
Level 1
  Adjacencies: 0, Priority: 64, Metric: 10
  Disabled
Level 2
  Adjacencies: 1, Priority: 64, Metric: 10
  Hello Interval: 20.000 s, Hold Time: 60 s
  Designated Router: nemean.03
show isis overview

Syntax

```
show isis overview
<instance instance-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches and QFX Series)

```
show isis overview
<instance instance-name>
```

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display IS-IS overview information.

Options

- **none**—Display standard overview information about IS-IS for all routing instances.
- **instance instance-name**—(Optional) Display overview information for the specified routing instance.
- **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 isis overview on page 2094`

Output Fields

Table 134 on page 2092 lists the output fields for the `show isis overview` command. Output fields are listed in the approximate order in which they appear.

**Table 134: show isis overview Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Name of the router.</td>
</tr>
<tr>
<td>Sysid</td>
<td>Part of the ISO address of the routing device.</td>
</tr>
<tr>
<td>Areaid</td>
<td>The area number of the routing device.</td>
</tr>
<tr>
<td>Instance</td>
<td>IS-IS routing instance.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the routing device.</td>
</tr>
<tr>
<td>Adjacency holddown</td>
<td>Adjacency holddown capability: enabled or disabled.</td>
</tr>
</tbody>
</table>
Table 134: show isis overview Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Areas</td>
<td>Maximum number of IS-IS areas advertised by the routing device.</td>
</tr>
<tr>
<td>LSP lifetime</td>
<td>Lifetime of the link-state PDU, in seconds.</td>
</tr>
<tr>
<td>Filter low life time LSPs up to</td>
<td>LSPs with a lifetime lower than this value are filtered out.</td>
</tr>
<tr>
<td>Attached bit evaluation</td>
<td>Attached bit capability: enabled or disabled.</td>
</tr>
<tr>
<td>SPF delay</td>
<td>Delay before performing consecutive shortest-path-first (SPF) calculations.</td>
</tr>
<tr>
<td>SPF holddown</td>
<td>Delay before performing additional SPF calculations after the maximum number of consecutive SPF calculations is reached.</td>
</tr>
<tr>
<td>SPF rapid runs</td>
<td>Maximum number of SPF calculations that can be performed in succession before the holddown timer begins.</td>
</tr>
<tr>
<td>Overload bit at startup is set</td>
<td>Overload bit capability is enabled.</td>
</tr>
<tr>
<td>Overload high metrics</td>
<td>Overload high metrics capability: enabled or disabled.</td>
</tr>
<tr>
<td>Allow internal prefix overloading</td>
<td>Allow internal prefixes to be advertised with high metric: enabled or disabled</td>
</tr>
<tr>
<td>Allow external prefix overloading</td>
<td>Allow external prefixes to be advertised with high metric: enabled or disabled</td>
</tr>
<tr>
<td>Overload timeout</td>
<td>Time period after which overload is reset and the time that remains before the timer is set to expire.</td>
</tr>
<tr>
<td>Traffic engineering</td>
<td>Traffic engineering capability: enabled or disabled.</td>
</tr>
<tr>
<td>Restart</td>
<td>Graceful restart capability: enabled or disabled.</td>
</tr>
<tr>
<td>Restart duration</td>
<td>Time period for complete reacquisition of IS-IS neighbors.</td>
</tr>
<tr>
<td>Helper mode</td>
<td>Graceful restart helper capability: enabled or disabled.</td>
</tr>
<tr>
<td>Level</td>
<td>IS-IS level:</td>
</tr>
<tr>
<td>IPv4 is enabled</td>
<td>IP Protocol version 4 capability is enabled.</td>
</tr>
<tr>
<td>IPv6 is enabled</td>
<td>IP Protocol version 6 capability is enabled.</td>
</tr>
</tbody>
</table>
Table 134: show isis overview Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro-loop avoidance</td>
<td>Micro-loop avoidance is enabled. Generally adjacent nodes converge faster than neighboring nodes causing traffic to loop. A route convergence delay is configured to avoid such micro loops.</td>
</tr>
<tr>
<td>Internal route preference</td>
<td>Preference value of internal routes.</td>
</tr>
<tr>
<td>External route preference</td>
<td>Preference value of external routes.</td>
</tr>
<tr>
<td>Prefix export limit</td>
<td>Number of prefixes allowed to be exported, as configured by the prefix-export-limit statement.</td>
</tr>
<tr>
<td>Prefix export count</td>
<td>Number of prefixes exported.</td>
</tr>
<tr>
<td>Wide area metrics enabled</td>
<td>Wide area metrics capability is enabled.</td>
</tr>
<tr>
<td>Narrow metrics enabled</td>
<td>Narrow metrics capability is enabled.</td>
</tr>
<tr>
<td>Adjacency holddown is active</td>
<td>IS-IS adjacencies come up one after another when adjacency holddown is enabled.</td>
</tr>
</tbody>
</table>

Sample Output

show isis overview

user@host> show isis overview

Instance: master
    Router ID: 10.255.107.183
    Hostname: pro-bng3-a
    Sysid: 0192.0168.0001
    Areaid: 49.0002
    Adjacency holddown: enabled
    Maximum Areas: 3
    LSP life time: 1200
    Filter low life time LSPs up to: 300
    Attached bit evaluation: enabled
    SPF delay: 200 msec, SPF holddown: 5000 msec, SPF rapid runs: 3
    Overload bit at startup is set
        Overload high metrics: disabled
        Allow route leaking: disabled
        Allow internal prefix overloading: enabled
        Allow external prefix overloading: enabled
        Overload timeout: 60 sec
    IPV4 is enabled, IPV6 is enabled
    Micro-loop avoidance: Enabled
        Method: Route Convergence Delay, Route convergence delay: 5000 msec
    Traffic engineering: enabled
    Restart: Disabled
    Helper mode: Enabled
    Level 1
<table>
<thead>
<tr>
<th>Internal route preference: 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>External route preference: 160</td>
</tr>
<tr>
<td>Wide metrics are enabled, Narrow metrics are enabled</td>
</tr>
<tr>
<td>Adjacency holddown is active</td>
</tr>
<tr>
<td>Level 2</td>
</tr>
<tr>
<td>Internal route preference: 18</td>
</tr>
<tr>
<td>External route preference: 165</td>
</tr>
<tr>
<td>Prefix export limit: 5, Prefix export count: 5</td>
</tr>
<tr>
<td>Wide metrics are enabled</td>
</tr>
<tr>
<td>Adjacency holddown is active</td>
</tr>
</tbody>
</table>

user@host> show isis overview logical-system R2

Instance: master
  Router ID: 192.168.0.2
  Hostname: pro-bng3-a-R2
  Sysid: 0192.0168.0002
  Areaid: 49.0002
  Adjacency holddown: enabled
  Maximum Areas: 3
  LSP life time: 1200
  Attached bit evaluation: enabled
  SPF delay: 200 msec, SPF holddown: 5000 msec, SPF rapid runs: 3
  IPv4 is enabled, IPv6 is enabled
  Traffic engineering: enabled
  Restart: Disabled
  Helper mode: Enabled

Level 1
  Internal route preference: 15
  External route preference: 160
  Prefix export count: 0
  Wide metrics are enabled, Narrow metrics are enabled

Level 2
  Internal route preference: 18
  External route preference: 165
  Prefix export count: 0
  Wide metrics are enabled, Narrow metrics are enabled

user@host> show isis overview logical-system R3

Instance: master
  Router ID: 192.168.0.3
  Hostname: pro-bng3-a-R3
  Sysid: 0192.0168.0003
  Areaid: 49.0002
  Adjacency holddown: enabled
  Maximum Areas: 3
  LSP life time: 1200
  Attached bit evaluation: enabled
  SPF delay: 200 msec, SPF holddown: 5000 msec, SPF rapid runs: 3
  IPv4 is enabled, IPv6 is enabled
  Traffic engineering: enabled
  Restart: Disabled
  Helper mode: Enabled

Level 1
  Internal route preference: 15
  External route preference: 160
  Prefix export count: 0
  Wide metrics are enabled, Narrow metrics are enabled

Level 2
<table>
<thead>
<tr>
<th>Internal route preference: 18</th>
</tr>
</thead>
<tbody>
<tr>
<td>External route preference: 165</td>
</tr>
<tr>
<td>Prefix export count: 0</td>
</tr>
<tr>
<td>Wide metrics are enabled, Narrow metrics are enabled</td>
</tr>
</tbody>
</table>
show isis route

**List of Syntax**

Syntax on page 2097
Syntax (EX Series Switches and QFX Series) on page 2097

**Syntax**

```
show isis route
<destination>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**Syntax (EX Series Switches and QFX Series)**

```
show isis route
<destination>
<inet | inet6>
<instance instance-name>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display the routes in the IS-IS routing table.

**Options**

```
none—Display all routes in the IS-IS routing table for all supported address families for all routing instances.
```

```
destination—(Optional) Destination address for the route.
```

```
inet | inet6—(Optional) Display inet (IPv4) or inet6 (IPv6) routes, respectively.
```

```
instance instance-name—(Optional) Display routes for the specified routing instance only.
```

```
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
```

```
topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)—(Optional) Display routes for the specified topology only, or use unicast to display information, if available, for both IPv4 and IPv6 unicast topologies.
```

**Required Privilege Level**

```
view
```

**List of Sample Output**

```
show isis route logical-system on page 2098
show isis route floodgroup on page 2099
show isis route (CLNS) on page 2099
```
**show isis route on page 2099**

**Output Fields**  Table 135 on page 2098 describes the output fields for the `show isis route` command. Output fields are listed in the approximate order in which they appear.

**Table 135: show isis route Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version</td>
<td>Number of the current version of the IS-IS routing table.</td>
</tr>
<tr>
<td>L1</td>
<td>Version of Level 1 SPF that was run.</td>
</tr>
<tr>
<td>L2</td>
<td>Version of Level 2 SPF that was run.</td>
</tr>
<tr>
<td>Prefix or Label</td>
<td>Destination of the route.</td>
</tr>
<tr>
<td>L</td>
<td>IS-IS level:</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
</tr>
<tr>
<td>Version</td>
<td>Version of SPF that generated the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric value associated with the route.</td>
</tr>
<tr>
<td>Type</td>
<td>Metric type: int (internal) or ext (external).</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface to the next hop.</td>
</tr>
<tr>
<td>Via</td>
<td>System identifier of the next hop, displayed as a name if possible.</td>
</tr>
<tr>
<td>ISO Routes</td>
<td>ISO routing table entries.</td>
</tr>
<tr>
<td>snpa</td>
<td>MAC address.</td>
</tr>
</tbody>
</table>

**Sample Output**

**show isis route logical-system**

```
user@host> show isis route logical-system ls1
IS-IS routing table             Current version: L1: 8 L2: 11
Prefix             L Version Metric Type Interface    Via
10.9.7.0/30        2      11     20 int  gr-0/2/0.0   h
10.9.201.1/32      2      11     60 int  gr-0/2/0.0   h
IPV6 Unicast IS-IS routing table             Current version: L1: 9 L2: 11
Prefix             L Version Metric Type Interface    Via
8009:3::a09:3200/126 2      11     20 int  gr-0/2/0.0   h
```
### show isis route floodgroup

```
user@R2> show isis route floodgroup 49.0001

IS-IS routing table            Current version: L1: 14 L2: 27
IPv4/IPv6 Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>L Version</th>
<th>Metric Type</th>
<th>Interface</th>
<th>NH</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>1</td>
<td>14</td>
<td>10 int ge-0/0/8.0</td>
<td>IPV4 R1</td>
<td></td>
</tr>
<tr>
<td>81.3.3.3/32</td>
<td>1</td>
<td>14</td>
<td>10 int ge-0/0/8.0</td>
<td>IPV4 R1</td>
<td></td>
</tr>
<tr>
<td>128.220.17.202/32</td>
<td>1</td>
<td>14</td>
<td>10 int ge-0/0/8.0</td>
<td>IPV4 R1</td>
<td></td>
</tr>
</tbody>
</table>
```

### show isis route (CLNS)

```
user@host> show isis route

IS-IS routing table            Current version: L1: 10 L2: 8
IPv4/IPv6 Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>L Version</th>
<th>Metric Type</th>
<th>Interface</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>1</td>
<td>10</td>
<td>10 int fe-0/0/1.0</td>
<td>ISIS.0</td>
</tr>
<tr>
<td>47.0005.80ff.f800.000.001.0001/104</td>
<td>1</td>
<td>10</td>
<td>10 int fe-0/0/1.0</td>
<td>ISIS.0 0:12:0:34:0:56</td>
</tr>
</tbody>
</table>

ISO Routes

| Prefix        | L Version | Metric Type | Interface       | Via          | snpa          |
|---------------|-----------|-------------|-----------------|--------------|
| 47.0005.80ff.f800.000.001.0001/104 | 1 | 10 | 10 int fe-0/0/1.0 | ISIS.0 0:12:0:34:0:56 |
| 47.0005.80ff.f800.000.001.0001.192.6800.4001/152 | 1 | 10 | 10 int fe-0/0/1.0 | ISIS.0 0:12:0:34:0:56 |
| 47.0005.80ff.f800.000.001.0001.192.6800.4002/152 | 1 | 10 | 20 int fe-0/0/1.0 | ISIS.0 0:12:0:34:0:56 |
| 47.0005.80ff.f800.000.001.0002/104 | 1 | 10 | 10 int fe-0/0/1.0 | ISIS.0 0:12:0:34:0:56 |
```

### show isis route

```
user@host> show isis route

IS-IS routing table            Current version: L1: 4 L2: 13
IPv4/IPv6 Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>L Version</th>
<th>Metric Type</th>
<th>Interface</th>
<th>NH</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.71.52/32</td>
<td>2</td>
<td>13</td>
<td>10 int ae0.0</td>
<td>IPV4 camaro</td>
<td></td>
</tr>
<tr>
<td>10.255.71.238/32</td>
<td>2</td>
<td>13</td>
<td>20 int so-6/0/0.0</td>
<td>IPV4 olympic</td>
<td></td>
</tr>
<tr>
<td>10.255.71.239/32</td>
<td>2</td>
<td>13</td>
<td>20 int so-6/0/0.0</td>
<td>IPV4 olympic</td>
<td></td>
</tr>
<tr>
<td>10.255.71.242/32</td>
<td>2</td>
<td>13</td>
<td>10 int as0.0</td>
<td>IPV4 glacier</td>
<td></td>
</tr>
<tr>
<td>10.255.71.243/32</td>
<td>2</td>
<td>13</td>
<td>10 int as0.0</td>
<td>IPV4 glacier</td>
<td></td>
</tr>
<tr>
<td>12.13.0.0/30</td>
<td>2</td>
<td>13</td>
<td>20 int so-6/0/0.0</td>
<td>IPV4 olympic</td>
<td></td>
</tr>
</tbody>
</table>
```
### Interfaces Fundamentals for Routing Devices

<table>
<thead>
<tr>
<th>Label</th>
<th>L Version</th>
<th>Metric Type</th>
<th>Interface</th>
<th>NH</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>300032 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.13</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>300048 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.12</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>300064 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.12</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>300080 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.12</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>300096 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.12</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>299920 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.14</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>299936 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.14</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>299952 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.14</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>299968 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.14</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
<tr>
<td>299984 /52</td>
<td>2</td>
<td>MPLS</td>
<td>lt-1/2/0.13</td>
<td>0 int</td>
<td>Direct forward</td>
</tr>
</tbody>
</table>

### MPLS Routes

<table>
<thead>
<tr>
<th>Label</th>
<th>L Version</th>
<th>Metric Type</th>
<th>Interface</th>
<th>NH</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.15.0.0/30</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV4 olympic</td>
</tr>
<tr>
<td>13.15.0.0/30</td>
<td>2</td>
<td>10 int</td>
<td>ae0.0</td>
<td>13</td>
<td>IPV4 camaro</td>
</tr>
<tr>
<td>13.16.0.0/30</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV4 olympic</td>
</tr>
<tr>
<td>14.15.0.0/30</td>
<td>2</td>
<td>10 int</td>
<td>ae0.0</td>
<td>13</td>
<td>IPV4 camaro</td>
</tr>
<tr>
<td>192.2.1.0/30</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV4 olympic</td>
</tr>
<tr>
<td>1eee::/64</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV6 olympic</td>
</tr>
<tr>
<td>abcd::10:255:71:52/128</td>
<td>2</td>
<td>10 int</td>
<td>ae0.0</td>
<td>13</td>
<td>IPV6 camaro</td>
</tr>
<tr>
<td>abcd::10:255:71:238/128</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV6 olympic</td>
</tr>
<tr>
<td>abcd::10:255:71:239/128</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV6 olympic</td>
</tr>
<tr>
<td>abcd::10:255:71:242/128</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV6 olympic</td>
</tr>
<tr>
<td>abcd::10:255:71:243/128</td>
<td>2</td>
<td>10 int</td>
<td>so-6/0/0.0</td>
<td>13</td>
<td>IPV6 olympic</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Prefix</th>
<th>RTT</th>
<th>MTU</th>
<th>Action</th>
<th>Intf</th>
<th>Protocol</th>
<th>Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>300000 /52</td>
<td>1</td>
<td>27</td>
<td>0 int  !t-1/2/0.13</td>
<td>MPLS</td>
<td>Direct forward</td>
<td></td>
</tr>
<tr>
<td>300016 /52</td>
<td>2</td>
<td>38</td>
<td>0 int  !t-1/2/0.13</td>
<td>MPLS</td>
<td>Direct forward</td>
<td></td>
</tr>
</tbody>
</table>

To 10.0.7.60 (pro-bng3-c-E)
show isis spf

**List of Syntax**

Syntax on page 2102  
Syntax (EX Series Switches) on page 2102

**Syntax**

```
show isis spf (brief | log | results)
<instance instance-name>
<level (1 | 2)>
<logical-system (all | logical-system-name)>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**Syntax (EX Series Switches)**

```
show isis spf (brief | log | results)
<instance instance-name>
<level (1 | 2)>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**Release Information**

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

**Description**

Display information about IS-IS shortest-path-first (SPF) calculations.

**Options**

- **brief**—Display an overview of SPF calculations.
- **log**—Display the log of SPF calculations.
- **results**—Display the results of SPF calculations.
- **instance instance-name**—(Optional) Display SPF calculations for the specified routing instance.
- **level (1 | 2)**—(Optional) Display SPF calculations for the specified IS-IS level.
- **log**—Display the log of SPF calculations.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **results**—Display the results of SPF calculations.
- **topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)**—(Optional) Display SPF calculations for the specified topology only.

**Required Privilege**

View

**List of Sample Output**

show isis spf log on page 2103  
show isis spf results logical-system on page 2104  
show isis spf results (CLNS) on page 2105
Output Fields

Table 136 on page 2103 describes the output fields for the `show isis spf` command. Output fields are listed in the approximate order in which they appear.

**Table 136: show isis spf Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>System ID of a node.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric to the node.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface of the next hop.</td>
</tr>
<tr>
<td>Via</td>
<td>System ID of the next hop.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
</tr>
<tr>
<td>Start time</td>
<td>(log option only) Time that the SPF computation started.</td>
</tr>
<tr>
<td>Elapsed (secs)</td>
<td>(log option only) Length of time, in seconds, required to complete the SPF computation.</td>
</tr>
<tr>
<td>Count</td>
<td>(log option only) Number of times the SPF was triggered.</td>
</tr>
<tr>
<td>Reason</td>
<td>(log option only) Reason that the SPF computation was completed.</td>
</tr>
</tbody>
</table>

Sample Output

show isis spf log

```
user@host> show isis spf log

IS-IS level 1 SPF log:

<table>
<thead>
<tr>
<th>Start time</th>
<th>Elapsed (secs)</th>
<th>Count</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000069</td>
<td>1</td>
<td>Reconfig</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000107</td>
<td>3</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000050</td>
<td>3</td>
<td>Address change on so-1/2/2.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:23</td>
<td>0.000033</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:28</td>
<td>0.000178</td>
<td>5</td>
<td>New adjacency scat on ge-1/1/0.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:59</td>
<td>0.000060</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:42:30</td>
<td>0.000161</td>
<td>3</td>
<td>New adjacency h on gr-0/2/0.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:54:37</td>
<td>0.000195</td>
<td>1</td>
<td>Periodic SPF</td>
</tr>
</tbody>
</table>

IS-IS level 2 SPF log:

<table>
<thead>
<tr>
<th>Start time</th>
<th>Elapsed (secs)</th>
<th>Count</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000035</td>
<td>1</td>
<td>Reconfig</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000047</td>
<td>2</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000043</td>
<td>5</td>
<td>Address change on gr-0/2/0.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:23</td>
<td>0.000022</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:59</td>
<td>0.000144</td>
<td>3</td>
<td>New adjacency h on gr-0/2/0.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:42:30</td>
<td>0.000257</td>
<td>3</td>
<td>New LSP skag.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:54:37</td>
<td>0.000195</td>
<td>1</td>
<td>Periodic SPF</td>
</tr>
<tr>
<td>Fri Oct 31 12:55:50</td>
<td>0.000178</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:55:55</td>
<td>0.000174</td>
<td>1</td>
<td>Updated LSP h.00-00</td>
</tr>
</tbody>
</table>
```
show isis spf results logical-system

user@host> show isis spf results logical-system ls1

IS-IS level 1 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>scat.00</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>10.9.1.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 nodes

IS-IS level 2 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>10.9.7.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>skag.02</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10.9.6.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>h.00</td>
<td>10</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>10.9.7.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>10.9.6.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>10.9.201.1/32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10.9.1.0/30</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10.9.5.0/30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show isis spf results (CLNS)

```
user@host> show isis spf results

IS-IS level 1 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
</tbody>
</table>

2 nodes

show isis spf results

```

---

**IPv6 Unicast IS-IS level 1 SPF results:**

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>scat.00</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td></td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
</tbody>
</table>

10 IPv6 Unicast IS-IS level 1 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>scat.00</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td></td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
</tbody>
</table>

**IPv6 Unicast IS-IS level 2 SPF results:**

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3:a09:3200/126</td>
</tr>
<tr>
<td>skag.02</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3:a09:3200/126</td>
</tr>
<tr>
<td>h.00</td>
<td>10</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3:a09:3200/126</td>
</tr>
</tbody>
</table>

3 IPv6 Unicast IS-IS level 2 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Multicast IS-IS level 1 SPF results:**

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>scat.00</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td></td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
</tbody>
</table>

3 Multicast IS-IS level 1 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td>skag.02</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
<tr>
<td>h.00</td>
<td>10</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td></td>
</tr>
</tbody>
</table>

4 Multicast IS-IS level 2 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>10.255.245.1/32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>192.168.37.64/29</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>47.0005.80ff.800.0000.0109.0010/104</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>10.255.245.1/32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>192.168.37.64/29</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 nodes
show isis statistics

List of Syntax  Syntax on page 2107
Syntax (EX Series Switches and QFX Series) on page 2107

Syntax  show isis statistics
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)  show isis statistics
<instance instance-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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Display statistics about IS-IS traffic.

Options  none—Display IS-IS traffic statistics for all routing instances.

instance instance-name—(Optional) Display statistics for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all
logical systems or on a particular logical system.

Required Privilege  view
Level

Related  • clear isis statistics on page 2052
Documentation

List of Sample Output  show isis statistics on page 2109

Output Fields  Table 137 on page 2108 describes the output fields for the show isis statistics command.
Output fields are listed in the approximate order in which they appear.
### Table 137: show isis statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PDU type</strong></td>
<td><strong>Field Description</strong></td>
</tr>
<tr>
<td>PDU type:</td>
<td><strong>Field Description</strong></td>
</tr>
<tr>
<td>• CSNP</td>
<td>Complete sequence number PDUs contain a complete list of all link-state PDUs in the IS-IS database. CSNPs are sent periodically on all links, and the receiving systems use the information in the CSNP to update and synchronize their link-state PDU databases. The designated router multicasts CSNPs on broadcast links in place of sending explicit acknowledgments for each link-state PDU.</td>
</tr>
<tr>
<td>• IIH</td>
<td>IS-IS hello packets are broadcast to discover the identity of neighboring IS-IS systems and to determine whether the neighbors are Level 1 or Level 2 intermediate systems.</td>
</tr>
<tr>
<td>• LSP</td>
<td>Link-state PDUs contain information about the state of adjacencies to neighboring IS-IS systems. Link-state PDUs are flooded periodically throughout an area.</td>
</tr>
<tr>
<td>• PSNP</td>
<td>Partial sequence number PDUs are sent multicast by a receiver when it detects that it is missing a link-state PDU.</td>
</tr>
<tr>
<td>• Unknown</td>
<td>The PDU type is unknown.</td>
</tr>
<tr>
<td><strong>Received</strong></td>
<td>Number of PDUs received since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Processed</strong></td>
<td>Number of PDUs received less the number dropped.</td>
</tr>
<tr>
<td><strong>Drops</strong></td>
<td>Number of PDUs dropped.</td>
</tr>
<tr>
<td><strong>Sent</strong></td>
<td>Number of PDUs transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Rexmit</strong></td>
<td>Number of PDUs retransmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Total packets received/sent</strong></td>
<td>Total number of PDUs received and transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>SNP queue length</strong></td>
<td>Number of CSPN and PSNP packets currently waiting in the queue for processing. This value is almost always 0.</td>
</tr>
<tr>
<td><strong>LSP queue length</strong></td>
<td>Number of link-state PDUs waiting in the queue for processing. This value is almost always 0.</td>
</tr>
<tr>
<td><strong>SPF runs</strong></td>
<td>Number of shortest-path-first (SPF) calculations that have been performed. If this number is incrementing rapidly, it indicates that the network is unstable.</td>
</tr>
<tr>
<td><strong>Fragments rebuilt</strong></td>
<td>Number of link-state PDU fragments that the local system has computed.</td>
</tr>
<tr>
<td><strong>LSP regenerations</strong></td>
<td>Number of link-state PDUs that have been regenerated. A link-state PDU is regenerated when it is nearing the end of its lifetime and it has not changed.</td>
</tr>
<tr>
<td><strong>Purges initiated</strong></td>
<td>Number of purges that the system initiated. A purge is initiated if the software decides that a link-state PDU must be removed from the network.</td>
</tr>
</tbody>
</table>

**Table 137: show isis statistics Output Fields**
### Sample Output

```bash
show isis statistics
```

```
user@host> show isis statistics

IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>12227</td>
<td>12227</td>
<td>0</td>
<td>8184</td>
<td>683</td>
</tr>
<tr>
<td>IIH</td>
<td>113808</td>
<td>113808</td>
<td>0</td>
<td>115817</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>198868</td>
<td>198868</td>
<td>0</td>
<td>198934</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>6985</td>
<td>6979</td>
<td>6</td>
<td>8274</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>331888</td>
<td>331882</td>
<td>6</td>
<td>331209</td>
<td>683</td>
</tr>
</tbody>
</table>

Total packets received: 331888 Sent: 331892

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 1014
Fragments rebuilt: 1038
LSP regenerations: 425
Purges initiated: 0
```
CHAPTER 22

LLDP Operational Commands

- clear lldp neighbors
- clear lldp statistics
- show lldp
- show lldp local-information
- show lldp neighbors
- show lldp remote-global-statistics
- show lldp statistics
### clear lldp neighbors

**Syntax**

```
clear lldp neighbor
<interface interface-name>
```

**Release Information**

**Description**
Clear information regarding all Link Layer Discovery Protocol (LLDP) neighbors or LLDP neighbors of the specified interface.

For information about interface names, see “Interface Naming Overview” on page 16. For information about interface names for TX Matrix routers, see *TX Matrix Router Chassis and Interface Names*. For information about FPC numbering on TX Matrix routers, see *Routing Matrix with a TX Matrix Router FPC Numbering*.

For information about interface names in the Junos Fusion technology, see *Understanding Junos Fusion Ports*.

**Options**

```
interface interface-name — (Optional) Clear the LLDP neighbors on the specified interface.
```

**Required Privilege Level**
clear

**Related Documentation**
- clear lldp statistics on page 2113

**List of Sample Output**
- clear lldp neighbors on page 2112
- clear lldp neighbors interface ge-0/1/1.0 on page 2112

**Output Fields**
When you enter this command, you are provided no feedback on the status of your request. You can enter the `show lldp neighbors` command before and after clearing the LLDP neighbors to verify the clear operation.

**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 neighbor
       <interface interface-name>


Description  Clear all Link Layer Discovery Protocols (LLDP) statistics or LLDP statistics associated
with the specified interface.

For information about interface names, see “Interface Naming Overview” on page 16. For
information about interface names for TX Matrix routers, see "TX Matrix Router Chassis and Interface Names."
For information about FPC numbering on TX Matrix routers, see "Routing Matrix with a TX Matrix Router FPC Numbering."

For information about interface names in the Junos Fusion technology, see "Understanding Junos Fusion Ports."

Options  interface interface-name—(Optional) Clear LLDP statistics on the specified interface.

Required Privilege  clear

Related Documentation  •  clear lldp neighbors on page 2112

List of Sample Output  clear lldp statistics on page 2113
                       clear lldp statistics interface ge-0/1/1.0 on page 2113

Output Fields  When you enter this command, you are provided no feedback on the status of your
request. You can enter the show lldp statistics command before and after clearing the
LLDP statistics to verify the clear operation.

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
show lldp

Syntax

show lldp
<detail>

Release Information


Description

Display information about the Link Layer Discovery Protocol (LLDP).

Options

detail—(Optional) Display the detailed output level.

Required Privilege

Level

view

List of Sample Output

show lldp on page 2116
show lldp detail on page 2116

Output Fields

Table 138 on page 2114 describes the output fields for the show lldp command. Output fields are listed in the approximate order in which they appear.

Table 138: show lldp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>Status of LLDP: Enabled or Disabled.</td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>Value of the advertisement interval parameter.</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>Value of the transmit delay parameter.</td>
</tr>
<tr>
<td>Hold timer</td>
<td>Value of the hold timer parameter.</td>
</tr>
<tr>
<td>Notification interval</td>
<td>Value of the notification interval parameter.</td>
</tr>
<tr>
<td>Config Trap interval</td>
<td>Value of the configuration trap parameter.</td>
</tr>
<tr>
<td>Connection Hold timer</td>
<td>Value of the connection hold timer parameter.</td>
</tr>
</tbody>
</table>
| Port ID TLV subtype | • interface-name—Indicates the interface name as the port information for the local device.  
                      • locally-assigned—Indicates that the sub-type for port ID TLV generation is locally assigned value of SNMP index of the interface.  
                      For more information about port ID TLV subtype, see port-id-subtype. |
Table 138: show lldp Output Fields  (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Description TLV type</td>
<td>Following value used for port description TLV:</td>
</tr>
<tr>
<td></td>
<td>• interface-alias (ifAlias)—Indicates that the ifAlias MIB object value is used to generate the port description TLV.</td>
</tr>
<tr>
<td></td>
<td>• interface-description (ifDescr)—Indicates that the ifDescr MIB object value is used to generate the port description TLV.</td>
</tr>
<tr>
<td></td>
<td>For more information about port description TLV type, see port-description-type.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface for which LLDP configuration information is being reported.</td>
</tr>
<tr>
<td></td>
<td>For information about interface names, see “Interface Naming Overview” on page 16. For information about interface names for TX Matrix routers, see TX Matrix Router Chassis and Interface Names. For information about FPC numbering on TX Matrix routers, see Routing Matrix with a TX Matrix Router FPC Numbering.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs.</td>
</tr>
<tr>
<td>LLDP</td>
<td>LLDP operating state. The state can be Enabled or Disabled.</td>
</tr>
<tr>
<td>LLDP-MED</td>
<td>LLDP-MED operating state. The state can be Enabled or Disabled.</td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>LLDP power negotiation operating state. The state can be Enabled or Disabled.</td>
</tr>
<tr>
<td>LLDP basic TLVs supported</td>
<td>List of basic LLDP TLVs supported by this device (detail only).</td>
</tr>
<tr>
<td>LLDP 802 TLVs supported</td>
<td>List of IEEE 802.1 LLDP TLVs supported by this device (detail only).</td>
</tr>
</tbody>
</table>
Sample Output

show lldp

```
user@host> 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
Port ID TLV subtype       : locally-assigned
Port Description TLV type : interface-description (ifDescr)

<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></td>
<td></td>
</tr>
</tbody>
</table>
```

Sample Output

show lldp detail

```
user@host> 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
Port ID TLV subtype       : locally-assigned
Port Description TLV type : interface-description (ifDescr)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-0/0/0</td>
<td>-</td>
<td>4080</td>
<td>vlan-4080</td>
</tr>
<tr>
<td>xe-0/0/1</td>
<td>-</td>
<td>4080</td>
<td>vlan-4080</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:
Port VLAN tag, VLAN Name, MAC/PHY Configuration/Status, Link Aggregation, Maximum Frame Size
```
**show lldp local-information**

**Syntax**

`show lldp local-information`

**Release Information**


**Description**

Display local Link Layer Discovery Protocol (LLDP) information.

**Options**

This command has no options.

**Required Privilege Level**

`view`

**List of Sample Output**

- `show lldp local-information (Management Information Address Subtype is IPv4)` on page 2119
- `show lldp local-information (Management Information Address Subtype is IPv6)` on page 2119

**Output Fields**

Table 139 on page 2117 describes the output fields for the `show lldp local-information` command. Output fields are listed in the approximate order in which they appear.

**Table 139: 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 that follows pertains to the local system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>List of chassis identifiers for local information.</td>
</tr>
<tr>
<td>System name</td>
<td>Local system name reported by LLDP.</td>
</tr>
<tr>
<td>System descr</td>
<td>Local system description reported by LLDP.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Capabilities (such as Bridge or Router) that are Supported or Enabled by system on the interface.</td>
</tr>
<tr>
<td>Management Information</td>
<td>Listed by Interface Name, Address Subtype (such as ipv4, ipv6), Address (such as 192.168.168.229, 1fd:1a10), Interface Number, and Interface Numbering Subtype.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>List of local interfaces. For information about interface names, see &quot;Interface Naming Overview&quot; on page 16. For information about interface names for TX Matrix routers, see TX Matrix Router Chassis and Interface Names. For information about FPC numbering on TX Matrix routers, see Routing Matrix with a TX Matrix Router FPC Numbering.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the ae interface to which the interface belongs</td>
</tr>
</tbody>
</table>
### Table 139: `show lldp local-information` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface ID</td>
<td>List of local interface identifiers.</td>
</tr>
<tr>
<td>Interface Description</td>
<td>List of local interface descriptions.</td>
</tr>
<tr>
<td>Status</td>
<td>List of interface conditions: UP or DOWN.</td>
</tr>
</tbody>
</table>
Sample Output

show lldp local-information(Management Information Address Subtype is IPv4)

user@host> show lldp local-information
LLDP Local Information details

Chassis ID   : 64:87:88:65:37:c0
System name  : apg-hp1

System Capabilities
  Supported       : Bridge Router
  Enabled         : Bridge Router

Management Information
  Interface Name : Unknown
  Address Subtype : IPv4(1)
  Address        : 10.216.97.103
  Interface Number : 1
  Interface Numbering Subtype : ifIndex(2)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Parent Interface</th>
<th>Interface ID</th>
<th>Interface description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpx0</td>
<td>-</td>
<td>1</td>
<td>fxp0</td>
<td>Up</td>
</tr>
<tr>
<td>me0</td>
<td>-</td>
<td>33</td>
<td>me0</td>
<td>Up</td>
</tr>
<tr>
<td>ge-2/0/0</td>
<td>ae0</td>
<td>1475</td>
<td>ge-2/0/0</td>
<td>Up</td>
</tr>
<tr>
<td>ge-2/0/1</td>
<td>ae0</td>
<td>1476</td>
<td>ge-2/0/1</td>
<td>Up</td>
</tr>
</tbody>
</table>

show lldp local-information(Management Information Address Subtype is IPv6)

user@host> show lldp local-information
LLDP Local Information details

Chassis ID   : ac:4b:c8:92:67:c0
System name  : apg-hp
System descr : Juniper Networks, Inc. mx240, version 13.2-20131210.0 [builder] Build date: 2013-12-10 06:23:15 UTC

System Capabilities
  Supported       : Bridge Router
  Enabled         : Bridge Router

Management Information
  Interface Name : fxp0
  Address Subtype : IPv6(2)
  Address        : 1fd::1a20
  Interface Number : 1
  Interface Numbering Subtype : ifIndex(2)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Parent Interface</th>
<th>Interface ID</th>
<th>Interface description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-2/0/4</td>
<td>-</td>
<td>530</td>
<td>-</td>
<td>Down</td>
</tr>
<tr>
<td>ge-1/2/5</td>
<td>-</td>
<td>531</td>
<td>-</td>
<td>Down</td>
</tr>
<tr>
<td>ge-2/0/2</td>
<td>-</td>
<td>528</td>
<td>ge-1/2/2</td>
<td>Up</td>
</tr>
<tr>
<td>ge-1/2/3</td>
<td>-</td>
<td>529</td>
<td>ge-1/2/3</td>
<td>Up</td>
</tr>
</tbody>
</table>
show lldp neighbors

Syntax

show lldp neighbors
<interface interface-name>
detail

Release Information

detail option introduced in Junos OS Release 19.1R2.

Description

Display information about LLDP neighbors.

For information about interface names, see “Interface Naming Overview” on page 16. For information about interface names for TX Matrix routers, see TX Matrix Router Chassis and Interface Names. For information about FPC numbering on TX Matrix routers, see Routing Matrix with a TX Matrix Router FPC Numbering.

For information about extended port names in the Junos Fusion technology, see Understanding Junos Fusion Ports.

Options

interface interface-name—(Optional) Display the neighbor information about a particular physical interface.

detail—(Optional) Display detailed information about LLDP neighbors.

NOTE: Starting with Junos OS Release 14.2, you can also display LLDP neighbor details for management interfaces, such as fxp or me, on MX Series routers.

Required Privilege Level

view

Related Documentation

• clear lldp neighbors on page 2112

List of Sample Output

show lldp neighbors interface ge-0/0/4 (Management Address is IPv4) on page 2124
show lldp neighbors interface ge-0/0/4 (Management Address is IPv6) on page 2124
show lldp neighbors (Management Ethernet Interfaces) on page 2124
show lldp neighbors detail on page 2126

Output Fields

Table 140 on page 2121 describes the output fields for the show lldp neighbors command. Output fields are listed in the approximate order in which they appear.
### Table 140: show lldp neighbors Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Remote Devices Information</td>
<td>Information about remote devices.</td>
</tr>
<tr>
<td>LocalInterface</td>
<td>List of local interfaces for which neighbor information is available.</td>
</tr>
<tr>
<td>ChassisID</td>
<td>List of chassis identifiers for neighbors.</td>
</tr>
<tr>
<td>PortInfo</td>
<td>List of port information gathered from neighbors. This could be the port identifier or port description.</td>
</tr>
<tr>
<td>SysName</td>
<td>List of system names gathered from neighbors.</td>
</tr>
<tr>
<td>LLDP Neighbor Information</td>
<td>Information about both local and neighbor systems on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Local Information</td>
<td>Information about local systems on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Neighbor Information</td>
<td>Information about both local and neighbor system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Index</td>
<td>Local interface index (appears when the interface option is used).</td>
</tr>
<tr>
<td>Time Mark</td>
<td>Date and timestamp of information (appears when the interface option is used).</td>
</tr>
<tr>
<td>Time To Live</td>
<td>Number of seconds for which this information is valid (appears when the interface option is used).</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the local physical interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the ae interface to which the interface belongs</td>
</tr>
<tr>
<td>Local Port ID</td>
<td>Local port identifier (appears when the interface option is used).</td>
</tr>
<tr>
<td>Neighbor Information</td>
<td>Information about neighbor systems 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 type listed (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port type</td>
<td>Type of port identifier supplied, such as local (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port identifier of type listed (appears when the interface option is used).</td>
</tr>
</tbody>
</table>
Table 140: show lldp neighbors Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<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 or router) that are Supported or Enabled by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Management address</td>
<td>Details of the management address: <strong>Address Type</strong> (such as ipv4 and ipv6), <strong>Address</strong> (such as 10.204.34.35, 1fd::1a10), <strong>Interface Number</strong>, <strong>Interface Subtype</strong>, and Organization Identifier (OID) (appears when the interface option is used).</td>
</tr>
<tr>
<td>Organization Info</td>
<td>One or more entries listing remote information by Organizationally Unique Identifier (OUI), <strong>Subtype</strong>, <strong>Index</strong>, and <strong>Info</strong> (appears when the interface option is used).</td>
</tr>
</tbody>
</table>

Table 141 on page 2122 describes the output fields for the show lldp neighbors detail command. Output fields are listed in the approximate order in which they appear.

Table 141: show lldp neighbors detail Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Neighbor Information</td>
<td>Information about all neighbors in the system.</td>
</tr>
<tr>
<td>Local Information</td>
<td>Information about neighbors on a local interface.</td>
</tr>
<tr>
<td>Index</td>
<td>Local interface index.</td>
</tr>
<tr>
<td>Time To Live</td>
<td>Number of seconds for which neighbor information is valid for this interface.</td>
</tr>
<tr>
<td>Time Mark</td>
<td>Date and timestamp information.</td>
</tr>
<tr>
<td>Age</td>
<td>Age (in seconds) of the neighbor since the TLV is received from the neighbor.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Local Interface for which the neighbor detail is displayed.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the ae interface to which the interface belongs</td>
</tr>
<tr>
<td>Local Port ID</td>
<td>Local port identifier.</td>
</tr>
<tr>
<td>Ageout Count</td>
<td>Number of times the neighbor information has been aged out on this interface.</td>
</tr>
</tbody>
</table>
### Table 14: show lldp neighbors detail 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 the neighbor systems.</td>
</tr>
<tr>
<td>Chassis type</td>
<td>Type of chassis identifier supplied, such as MAC address.</td>
</tr>
<tr>
<td>Chassisid</td>
<td>List of chassis identifiers for all neighbors in the system.</td>
</tr>
<tr>
<td>Port type</td>
<td>Capabilities (such as bridge or router) that are Supported or Enabled by the system.</td>
</tr>
<tr>
<td>Port description</td>
<td>Port description.</td>
</tr>
<tr>
<td>System name</td>
<td>Name supplied by the system.</td>
</tr>
<tr>
<td>System Description</td>
<td>Description supplied by the system.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Capabilities (such as bridge or router) that are Supported or Enabled by the system.</td>
</tr>
<tr>
<td>Management address</td>
<td>Details about the management address and management interface of the neighbor.</td>
</tr>
<tr>
<td>Media endpoint class</td>
<td>LLDP MED device class value of the neighbor system.</td>
</tr>
<tr>
<td>Organization Info</td>
<td>One or more entries listing the organization-specific TLV sent by the neighbor.</td>
</tr>
</tbody>
</table>
Sample Output

show lldp neighbors interface ge-0/0/4 (Management Address is IPv4)

user@host> show lldp neighbors interface ge-0/0/4

LLDP Neighbor Information:
Local Information:
  Index: 2 Time to live: 120 Time mark: Tue Dec 31 11:47:46 2013 Age: 15 secs
  Local Interface    : ge-2/0/1
  Parent Interface   : ae0
  Local Port ID      : 1476
  Ageout Count      : 0

Neighbour Information:
  Chassis type       : Mac address
  Chassis ID         : ac:4b:c8:92:67:c0
  Port type          : Locally assigned
  Port ID            : 529
  Port description   : ge-1/2/3
  System name        : apg-hp

  System Description : Juniper Networks, Inc. mx240 , version 14.1-20131222.0
  [builder] Build date: 2013-12-22 09:13:26 UTC

  System capabilities
    Supported: Bridge Router
    Enabled  : Bridge Router

  Management address
    Address Type      : IPv4(1)
    Address           : 10.216.98.57
    Interface Number  : 1
    Interface Subtype : ifIndex(2)
    OID               : 1.3.6.1.2.1.31.1.1.1.1.1.

  Organization Info
    OUI      : IEEE 802.3 Private (0x00120f)
    Subtype  : MACPHY Configuration/Status (1)
    Info     : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x1d), MAU Type (0x0)
    Index    : 1

  Organization Info
    OUI      : IEEE 802.3 Private (0x00120f)
    Subtype  : Link Aggregation (3)
    Info     : Aggregation Status (0x3), Aggregation Port ID (1694498816)
    Index    : 2

  Organization Info
    OUI      : IEEE 802.3 Private (0x00120f)
    Subtype  : Maximum Frame Size (4)
    Info     : MTU Size (1518)
    Index    : 3

show lldp neighbors interface ge-0/0/4 (Management Address is IPv6)

user@host> show lldp neighbors interface ge-0/0/4
LLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 120 Time mark: Thu Dec 12 07:19:45 2013 Age: 28 secs
Local Interface : ge-1/2/2
Parent Interface : -
Local Port ID : 528
Ageout Count : 0

Neighbour Information:
Chassis type : Mac address
Chassis ID : 64:87:88:65:37:c0
Port type : Locally assigned
Port ID : 1475
Port description : ge-2/0/0
System name : apg-hp1

System Description : Juniper Networks, Inc. mx240 , version 11.4R10 Build date: 2013-10-24 10:10:02 UTC

System capabilities
  Supported: Bridge Router
  Enabled : Bridge Router

Management address
  Address Type : IPv6(2)
  Address : 1fd::1a10
  Interface Number : 1
  Interface Subtype : ifIndex(2)
  OID : 1.3.6.1.2.1.31.1.1.1.1.1.

Organization Info
  OUI : IEEE 802.3 Private (0x00120f)
  Subtype : MAC/PHY Configuration/Status (1)
    Info : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x5), MAU Type (0x0)
    Index : 1

Organization Info
  OUI : IEEE 802.3 Private (0x00120f)
  Subtype : Link Aggregation (3)
    Info : Aggregation Status (0x1), Aggregation Port ID (0)
    Index : 2

Organization Info
  OUI : IEEE 802.3 Private (0x00120f)
  Subtype : Maximum Frame Size (4)
    Info : MTU Size (1518)
    Index : 3

Organization Info
  OUI : Ethernet Bridged (0x0080c2)
  Subtype : VLAN Name (3)
    Info : VLAN ID (100), VLAN Name (vlan-100)
    Index : 4

show lldp neighbors (Management Ethernet Interfaces)

user@host> show lldp neighbors
show lldp neighbors detail

user@host> show lldp neighbors detail

LLDP Neighbor Information:
Local Information:
Index: 1 Time to live: 120 Time mark: Wed Apr  3 08:25:57 2019 Age: 8 secs
Local Interface : me0
Parent Interface : -
Local Port ID : 33
Ageout Count : 0

Neighbour Information:
Chassis type : Mac address
Port type : Locally assigned
Port ID : 517
Port description : ge-0/0/7.0
System name : test

System Description : Juniper Networks, Inc. ex3300-48t , version 12.3R Build date: 2014-03-13 07:02:54 UTC

System capabilities
  Supported: Bridge Router
  Enabled  : Bridge Router

Management address
  Address Type : IPv4(1)
  Address : 10.221.0.111
  Interface Number : 34
  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 : IEEE 802.3 Private (0x00120f)
  Subtype : MAC/PHY Configuration/Status (1)
  Info : Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x6c11), MAU Type (0x0)
  Index : 1

Organization Info
  OUI : IEEE 802.3 Private (0x00120f)
  Subtype : Link Aggregation (3)
  Info : Aggregation Status [supported, disabled (0x1)], Aggregation Port ID (0)
  Index : 2
Organization Info
- OUI : IEEE 802.3 Private (0x00120f)
- Subtype : Maximum Frame Size (4)
- Info : MTU Size (1514)
- Index : 3

Organization Info
- OUI : Ethernet Bridged (0x0080c2)
- Subtype : Port Vid (1)
- Info : VLAN ID (52),
- Index : 4

Organization Info
- OUI : Juniper Specific (0x009069)
- Subtype : Chassis Serial Type (1)
- Info : Juniper Slot Serial [GA0215270535]
- Index : 5

Organization Info
- OUI : Ethernet Bridged (0x0080c2)
- Subtype : VLAN Name (3)
- Info : VLAN ID (52), VLAN Name (vlan52)
- Index : 6

LLDP Neighbor Information:
Local Information:
- Local Interface : ge-0/0/2
- Parent Interface : -
- Local Port ID : 512
- Ageout Count : 0

Neighbour Information:
- Chassis type : Mac address
- Port type : Locally assigned
- Port ID : 511
- Port description : ge-0/0/2

System Description : Juniper Networks, Inc. ex4300-24p Ethernet Switch, kernel JUNOS 17.1, Build date: 2019-03-26 08:12:13 UTC Copyright (c) 1996-2019 Juniper Networks, Inc.

System capabilities
- Supported: Bridge Router
- Enabled : Bridge Router

Management address
- Address Type : IPv4(1)
- Address : 10.204.39.247
- Interface Number : 33
- Interface Subtype : ifIndex(2)
- OID : 1.3.6.1.2.1.1.1.1.1.133.

Media endpoint class: Network Connectivity

Organization Info
- OUI : IEEE 802.3 Private (0x00120f)
<table>
<thead>
<tr>
<th>Subtype</th>
<th>Info</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC/PHY Configuration/Status (1)</td>
<td>Autonegotiation [supported, enabled (0x3)], PMD Autonegotiation Capability (0x1), MAU Type (0x0)</td>
<td>1</td>
</tr>
<tr>
<td>Organization Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUI</td>
<td>IEEE 802.3 Private (0x00120f)</td>
<td></td>
</tr>
<tr>
<td>Subtype</td>
<td>MDI Power (2)</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>MDI Power Support [PSE bit set, supported, disabled, CONTROL bit not set (0x3)], MDI Power Pair [signal], MDI Power Class [class1 (1)]</td>
<td>2</td>
</tr>
<tr>
<td>Organization Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUI</td>
<td>IEEE 802.3 Private (0x00120f)</td>
<td></td>
</tr>
<tr>
<td>Subtype</td>
<td>Link Aggregation (3)</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>Aggregation Status [supported, enabled (0x3)], Aggregation Port ID (556)</td>
<td>3</td>
</tr>
<tr>
<td>Organization Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUI</td>
<td>IEEE 802.3 Private (0x00120f)</td>
<td></td>
</tr>
<tr>
<td>Subtype</td>
<td>Maximum Frame Size (4)</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>MTU Size (6500)</td>
<td>4</td>
</tr>
<tr>
<td>Organization Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUI</td>
<td>IEEE 802.3 Private (0x00120f)</td>
<td></td>
</tr>
<tr>
<td>Subtype</td>
<td>Chassis Serial Type (1)</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>Juniper Slot Serial [MS3112240002]</td>
<td>5</td>
</tr>
<tr>
<td>Organization Info</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OUI</td>
<td>Ethernet Bridged (0x0080c2)</td>
<td></td>
</tr>
<tr>
<td>Subtype</td>
<td>VLAN Name (3)</td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td>VLAN ID (100), VLAN Name (vlan-100)</td>
<td>6</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Index</td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
show lldp remote-global-statistics

Syntax

show lldp remote-global-statistics

Release Information


Description

Display remote Link Layer Discovery Protocol (LLDP) global statistics.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show lldp remote-global-statistics on page 2130

Output Fields

Table 142 on page 2129 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 142: 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>
<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

```
user@host> show lldp remote-global-statistics

LLDP Remote Database Table Counters
LastchangeTime    Inserts    Deletes    Drops    Ageouts
00:00:76 (76 sec)    192        0          0        0
```


show lldp statistics

Syntax

show lldp statistics
<interface interface-name>

Release Information


Description

Display information about Link Layer Discovery Protocol (LLDP) statistics.

Options

interface interface-name—(Optional) Display the statistics about a particular physical interface.

NOTE: Starting with Junos OS Release 14.2, you can also display LLDP statistical details for management interfaces, such as fxp or me, on MX Series routers.

Required Privilege

Level view

Related Documentation

• clear lldp statistics on page 2113

List of Sample Output

show lldp statistics on page 2133
show lldp statistics interface ge-0/1/1 on page 2133

Output Fields

Table 143 on page 2131 describes the output fields for the show lldp statistics command. Output fields are listed in the approximate order in which they appear.

Table 143: show lldp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of LLDP frames received on this interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Number of LLDP frames sent on this interface.</td>
</tr>
</tbody>
</table>

For information about interface names, see “Interface Naming Overview” on page 16. For information about interface names for TX Matrix routers, see TX Matrix Router Chassis and Interface Names. For information about FPC numbering on TX Matrix routers, see Routing Matrix with a TX Matrix Router FPC Numbering.

For information about extended port names in the Junos Fusion technology, see Understanding Junos Fusion Ports.
Table 143: show lldp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown-TLVs</td>
<td>Number of LLDP frames with unsupported content received on this interface.</td>
</tr>
<tr>
<td>With-Errors</td>
<td>Number of LLDP frames with errors received on this interface.</td>
</tr>
<tr>
<td>Discarded</td>
<td>Number of LLDP frames received on this interface that were discarded because of problems.</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@host> 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>

Discarded TLVs  Transmitted  Untransmitted
0               3044         1
0               3044         1
0               3044         1
0               3044         1
0               3075         1
0               3075         1
0               3075         1
0               17312        0
0               17312        0
```

Sample Output

show lldp statistics interface ge-0/1/1

```
user@host> show lldp statistics interface ge-0/1/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Transmitted</th>
<th>Untransmitted</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
<th>Discarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/1/1</td>
<td>544</td>
<td>540</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
CHAPTER 23

MVRP Operational Commands

- show mvrp
- show mvrp applicant-state
- show mvrp dynamic-vlan-memberships
- show mvrp interface
- show mvrp registration-state
- show mvrp statistics
**show mvrp**

Syntax  

```
show mvrp
```

**Release Information**  
Command introduced in Junos OS Release 10.0 for EX Series switches.  
Command introduced in Junos OS Release 10.1 for MX Series routers.  
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

**Description**  
Display Multiple VLAN Registration Protocol (MVRP) configuration information.

**Required Privilege Level**  
view

**Related Documentation**  
- **Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches**
- **Verifying That MVRP Is Working Correctly on Switches**
  - show mvrp statistics on page 2148
  - show mvrp applicant-state on page 2139
  - show mvrp dynamic-vlan-memberships on page 2142
  - show mvrp interface on page 2144
  - show mvrp registration-state on page 2146
  - show mvrp statistics on page 2148
  - show mvrp applicant-state on page 2139
  - show mvrp dynamic-vlan-memberships on page 2142
  - show mvrp interface on page 2144
  - show mvrp registration-state on page 2146

**List of Sample Output**  
- `show mvrp (EX Series switches and MX Series routers) on page 2137`
- `show mvrp (SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320) on page 2137`
- `show mvrp (EX Series switches) on page 2138`

**Output Fields**  
`Table 144 on page 2136 lists the output fields for the show mvrp 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>MVRP dynamic VLAN creation</td>
<td>Displays whether global MVRP dynamic VLAN creation is <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
</tbody>
</table>
Table 144: show mvrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global MVRP configuration</td>
<td>Displays global MVRP information:</td>
</tr>
<tr>
<td></td>
<td>• MVRP status—Displays whether MVRP is Enabled or Disabled.</td>
</tr>
<tr>
<td></td>
<td>• MVRP dynamic vlan creation—Displays whether global MVRP dynamic VLAN creation is Disabled or Enabled.</td>
</tr>
<tr>
<td>MVRP BPDU MAC address</td>
<td>Displays the multicast media access control (MAC) address for MVRP. If configured, the provider MVRP multicast MAC address is used; otherwise, the customer MVRP multicast MAC address is used.</td>
</tr>
<tr>
<td>MVRP timers (ms)</td>
<td>Displays MVRP timer information:</td>
</tr>
<tr>
<td></td>
<td>• Interface—The interface on which MVRP is configured.</td>
</tr>
<tr>
<td></td>
<td>• Join—The maximum number of milliseconds the interfaces must wait before sending VLAN advertisements.</td>
</tr>
<tr>
<td></td>
<td>• Leave—The number of milliseconds an interface must wait after receiving a Leave message to remove the interface from the VLAN specified in the message.</td>
</tr>
<tr>
<td></td>
<td>• LeaveAll—The interval at which LeaveAll messages are sent on interfaces. LeaveAll messages maintain current MVRP VLAN membership information in the network.</td>
</tr>
<tr>
<td>Interface based configuration</td>
<td>Displays interface-specific MVRP information:</td>
</tr>
<tr>
<td></td>
<td>• Interface—The interface on which MVRP is configured.</td>
</tr>
<tr>
<td></td>
<td>• Status—Displays whether MVRP is Enabled or Disabled.</td>
</tr>
<tr>
<td></td>
<td>• Registration—Displays whether registration for the interface is Forbidden or Normal.</td>
</tr>
<tr>
<td></td>
<td>• Dynamic VLAN Creation—Displays whether interface dynamic VLAN creation is Enabled or Disabled.</td>
</tr>
</tbody>
</table>

Sample Output

show mvrp (EX Series switches and MX Series routers)

```
user@host> show mvrp
MVRP configuration for routing instance 'default-switch'
MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)
MVRP timers (ms)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Join</th>
<th>Leave</th>
<th>LeaveAll</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/2/8</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
<tr>
<td>ge-11/0/9</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
<tr>
<td>ge-11/3/0</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
</tbody>
</table>
```

Sample Output

show mvrp (SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320)

```
user@host> show mvrp
MVRP configuration for routing instance 'default-switch'
MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (00-00-5E-00-53-00)
MVRP timers (ms)
```
## Sample Output

### show mvrp (EX Series switches)

```
user@switch> show mvrp

Global MVRP configuration
MVRP status               : Enabled
MVRP dynamic vlan creation: Enabled
MVRP Timers (ms):
  Interface        Join   Leave   LeaveAll
  --------------- ----   -----   --------
  all              200    600     10000
  xe-0/1/1.0       200    600     10000

Interface based configuration:
  Interface          Status     Registration   Dynamic VLAN Creation
  ---------------   --------   ------------   ---------------------
  all       Disabled   Normal    Enabled
  xe-0/1/1.0     Enabled    Normal         Enabled
```
show mvrp applicant-state

Syntax

show mvrp applicant-state

Release Information

Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

Description

For MX Series routers, EX Series switches, SRX1500, SRX300, SRX550M, SRX345, SRX340, and SRX320, display Multiple VLAN Registration Protocol (MVRP) applicant state information.

Required Privilege Level

view

Related Documentation

- show mvrp on page 2136
- show mvrp interface on page 2144
- show mvrp registration-state on page 2146
- show mvrp statistics on page 2148
- show mvrp interface on page 2144
- show mvrp registration-state on page 2146

List of Sample Output

show mvrp applicant-state (EX Series and MX Series) on page 2140
show mvrp applicant-state on page 2140

Output Fields

Table 145 on page 2139 lists the output fields for the show mvrp applicant-state command. Output fields are listed in the approximate order in which they appear.

Table 145: show mvrp applicant-state Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>Displays the VLAN ID number.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the interface number associated with the VLAN ID.</td>
</tr>
</tbody>
</table>
Table 145: `show mvrp applicant-state` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays one of the following MVRP registrar states:</td>
</tr>
<tr>
<td></td>
<td>• VO—Very anxious observer.</td>
</tr>
<tr>
<td></td>
<td>• VP—Very anxious passive.</td>
</tr>
<tr>
<td></td>
<td>• VA—Very anxious new.</td>
</tr>
<tr>
<td></td>
<td>• AN—Anxious new.</td>
</tr>
<tr>
<td></td>
<td>• AA—Anxious active.</td>
</tr>
<tr>
<td></td>
<td>• QA—Quiet active.</td>
</tr>
<tr>
<td></td>
<td>• LA—Leaving active.</td>
</tr>
<tr>
<td></td>
<td>• AO—Anxious observer.</td>
</tr>
<tr>
<td></td>
<td>• QO—Quiet observer.</td>
</tr>
<tr>
<td></td>
<td>• LO—Leaving observer.</td>
</tr>
<tr>
<td></td>
<td>• AP—Anxious passive.</td>
</tr>
<tr>
<td></td>
<td>• QA—Quiet passive.</td>
</tr>
</tbody>
</table>

Sample Output (EX Series and MX Series)

`show mvrp applicant-state` (EX Series and MX Series)

```
user@host> show mvrp applicant-state

MVRP applicant state for routing instance 'default-switch'
(VO) Very anxious observer, (VP) Very anxious passive, (VA) Very anxious new,
(AN) Anxious new, (AA) Anxious active, (QA) Quiet active, (LA) Leaving active,
(AO) Anxious observer, (QO) Quiet observer, (LO) Leaving observer,
(AP) Anxious passive, (QP) Quiet passive

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>ge-11/3/0</td>
<td>Declaring (QA)</td>
</tr>
<tr>
<td>200</td>
<td>ge-11/3/0</td>
<td>Declaring (QA)</td>
</tr>
<tr>
<td>300</td>
<td>ge-11/3/0</td>
<td>Declaring (QA)</td>
</tr>
</tbody>
</table>
```

Sample Output (SRX1500, SRX300, SRX550M, SRX345, SRX340, and SRX320)

`show mvrp applicant-state`

```
user@host> show mvrp applicant-state

MVRP applicant state for routing instance 'default-switch'
(VO) Very anxious observer, (VP) Very anxious passive, (VA) Very anxious new,
(AN) Anxious new, (AA) Anxious active, (QA) Quiet active, (LA) Leaving active,
(AO) Anxious observer, (QO) Quiet observer, (LO) Leaving observer,
(AP) Anxious passive, (QP) Quiet passive

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ge-0/0/1</td>
<td>Idle (VO)</td>
</tr>
<tr>
<td>30</td>
<td>ge-0/0/1</td>
<td>Idle (VO)</td>
</tr>
<tr>
<td>40</td>
<td>ge-0/0/1</td>
<td>Idle (VO)</td>
</tr>
<tr>
<td>50</td>
<td>ge-0/0/1</td>
<td>Idle (VO)</td>
</tr>
<tr>
<td>100</td>
<td>ge-0/0/1</td>
<td>Idle (VO)</td>
</tr>
</tbody>
</table>
```
**show mvrp dynamic-vlan-memberships**

**Syntax**

`show mvrp dynamic-vlan-memberships`

**Release Information**

Command introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 10.1 for MX Series routers.
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

**Description**

Display all VLANs that have been created dynamically using Multiple VLAN Registration Protocol (MVRP) on the router, switch, or SRX Series device.

**Required Privilege**

`clear`

**Related Documentation**

- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches
- Verifying That MVRP Is Working Correctly on Switches
- `show mvrp` on page 2136
- `show mvrp applicant-state` on page 2139
- `show mvrp interface` on page 2144
- `show mvrp registration-state` on page 2146
- `show mvrp registration-state` on page 2146
- `show mvrp statistics` on page 2148

**List of Sample Output**

- `show mvrp dynamic-vlan-memberships (MX Series and EX Series)` on page 2143
- `show mvrp dynamic-vlan-memberships (EX Series)` on page 2143
- `show mvrp dynamic-vlan-memberships` on page 2143

**Output Fields**

Table 146 on page 2142 lists the output fields for the `show mvrp dynamic-vlan-memberships` command on MX Series routers and EX Series switches. Output fields are listed in the approximate order in which they appear.

**Table 146: show mvrp dynamic-vlan-memberships Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>The VLAN ID of the dynamically created VLAN.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The interface or interfaces that are bound to the dynamically created VLAN.</td>
</tr>
</tbody>
</table>
Sample Output (MX Series Routers and EX Series Switches)

show mvrp dynamic-vlan-memberships (MX Series and EX Series)

```
user@host> show mvrp dynamic-vlan-memberships
MVRP dynamic vlans for routing instance 'default-switch'
     (s) static vlan, (f) fixed registration

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 (s)</td>
<td>ge-11/3/0</td>
</tr>
<tr>
<td>200 (s)</td>
<td>ge-11/3/0</td>
</tr>
<tr>
<td>300 (s)</td>
<td></td>
</tr>
</tbody>
</table>
```

Sample Output (EX Series Switches)

show mvrp dynamic-vlan-memberships (EX Series)

```
user@switch> show mvrp dynamic-vlan-memberships

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mvrp_100</strong></td>
<td>xe-0/1/1.0</td>
</tr>
<tr>
<td></td>
<td>xe-0/1/0.0</td>
</tr>
<tr>
<td><strong>mvrp_200</strong></td>
<td>xe-0/1/1.0</td>
</tr>
<tr>
<td></td>
<td>xe-0/1/0.0</td>
</tr>
<tr>
<td><strong>mvrp_300</strong></td>
<td>xe-0/1/1.0</td>
</tr>
</tbody>
</table>
```

Sample Output (SRX1500, SRX300, SRX550M, SRX345, SRX340, SRX320)

show mvrp dynamic-vlan-memberships

```
user@host> show mvrp dynamic-vlan-memberships
MVRP dynamic vlans for routing instance 'default-switch'
     (s) static vlan, (f) fixed registration

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (s)</td>
<td></td>
</tr>
<tr>
<td>30 (s)</td>
<td></td>
</tr>
<tr>
<td>40 (s)</td>
<td>ge-0/0/1</td>
</tr>
<tr>
<td>50 (s)</td>
<td>ge-0/0/1</td>
</tr>
<tr>
<td>100 (s)</td>
<td>ge-0/0/1 (f)</td>
</tr>
</tbody>
</table>
```
show mvrp interface

Syntax
show mvrp interface

Release Information
Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

Description
Display Multiple VLAN Registration Protocol (MVRP) interface-specific information.

Required Privilege
Level: view

Related Documentation
• show mvrp on page 2136
• show mvrp applicant-state on page 2139
• show mvrp dynamic-vlan-memberships on page 2142
• show mvrp registration-state on page 2146
• show mvrp registration-state on page 2146
• show mvrp statistics on page 2148

List of Sample Output
show mvrp interface on page 2144
show mvrp interface on page 2145

Output Fields
Table 147 on page 2144 lists the output fields for the show mvrp interface command. Output fields are listed in the approximate order in which they appear.

Table 147: show mvrp 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 MVRP is configured.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the MVRP: Enabled or Disabled.</td>
</tr>
<tr>
<td>Registration Mode</td>
<td>Registration for the interface: Fixed, Forbidden, or Normal.</td>
</tr>
<tr>
<td>Applicant Mode</td>
<td>Applicant mode.</td>
</tr>
</tbody>
</table>

Sample Output (MX Series Routers and SX Series Switches)

show mvrp interface

user@host> show mvrp interface
MVRP interface information for routing instance 'default-switch'
### Sample Output (SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320)

show mvrp interface

```
user@host> show mvrp interface
MVRP interface information for routing instance 'default-switch'

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Registration Mode</th>
<th>Applicant Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>Normal</td>
<td>Normal</td>
</tr>
</tbody>
</table>
```
**show mvrp registration-state**

Syntax:  
```
show mvrp registration-state
```

**Release Information**  
Command introduced in Junos OS Release 10.1.  
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

**Description**  
For MX Series routers, EX Series switches and SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320, display Multiple VLAN Registration Protocol (MVRP) registration state information.

**Required Privilege**  
Level view

**Related Documentation**  
- show mvrp on page 2136  
- show mvrp dynamic-vlan-memberships on page 2142  
- show mvrp interface on page 2144  
- show mvrp statistics on page 2148

**List of Sample Output**  
show mvrp registration-state (EX Series and MX Series) on page 2147  
show mvrp registration-state (SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320) on page 2147

**Output Fields**  
Table 148 on page 2146 lists the output fields for the `show mvrp registration-state` command. Output fields are listed in the approximate order in which they appear.

**Table 148: show mvrp registration-state Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>Displays the VLAN ID number.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the interface number associated with the VLAN ID.</td>
</tr>
<tr>
<td>Registrar State</td>
<td>Displays whether the registrar state is Registered or Empty.</td>
</tr>
<tr>
<td>Forced State</td>
<td>Displays whether the forced state is Registered or Empty.</td>
</tr>
<tr>
<td>Managed State</td>
<td>Displays one of the following states:</td>
</tr>
<tr>
<td></td>
<td>• fixed — VLANs always stay in a registered state and are declared as such on all other forwarding ports.</td>
</tr>
<tr>
<td></td>
<td>• normal — VLANs participate in the MVRP protocol and honor incoming join requests normally.</td>
</tr>
<tr>
<td></td>
<td>• forbidden — VLANs ignore the incoming join requests and always stay in an unregistered state.</td>
</tr>
<tr>
<td>STP State</td>
<td>Displays whether the Spanning Tree Protocol (STP) is Blocking or Forwarding.</td>
</tr>
</tbody>
</table>
### Sample Output

**show mvrp registration-state (EX Series and MX Series)**

```
user@host> show mvrp registration-state

MVRP registration state for routing instance 'default-switch'

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interface</th>
<th>Registrar</th>
<th>Forced</th>
<th>Managed</th>
<th>STP</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>ge-11/2/8</td>
<td>Empty</td>
<td>Registered</td>
<td>Fixed</td>
<td>Forwarding</td>
</tr>
<tr>
<td></td>
<td>ge-11/0/9</td>
<td>Empty</td>
<td>Empty</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td></td>
<td>ge-11/3/0</td>
<td>Registered</td>
<td>Registered</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td>101</td>
<td>ge-11/2/8</td>
<td>Empty</td>
<td>Registered</td>
<td>Fixed</td>
<td>Forwarding</td>
</tr>
<tr>
<td></td>
<td>ge-11/0/9</td>
<td>Empty</td>
<td>Empty</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td></td>
<td>ge-11/3/0</td>
<td>Registered</td>
<td>Registered</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>
```

### Sample Output

**show mvrp registration-state (SRX1500, SRX300, SRX550M, SRX345, SRX340 and SRX320)**

```
user@host> show mvrp registration-state

MVRP registration state for routing instance 'default-switch'

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interface</th>
<th>Registrar</th>
<th>Forced</th>
<th>Managed</th>
<th>STP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ge-0/0/1</td>
<td>Empty</td>
<td>Empty</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td>30</td>
<td>ge-0/0/1</td>
<td>Empty</td>
<td>Empty</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td>40</td>
<td>ge-0/0/1</td>
<td>Registered</td>
<td>Registered</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td>50</td>
<td>ge-0/0/1</td>
<td>Registered</td>
<td>Registered</td>
<td>Normal</td>
<td>Forwarding</td>
</tr>
<tr>
<td>100</td>
<td>ge-0/0/1</td>
<td>Empty</td>
<td>Registered</td>
<td>Fixed</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>
```
show mvrp statistics

List of Syntax

Syntax (EX Series Switches) on page 2148
Syntax (Switches with ELSS Support) on page 2148
Syntax (SRX Devices) on page 2148

Syntax (EX Series Switches)

```
show mvrp statistics
<interface interface-name>
```

Syntax (Switches with ELSS Support)

```
show mvrp statistics
<interface interface-name>
<routing-instance routing-instance-name>
```

Syntax (SRX Devices)

```
show mvrp statistics
```

Release Information

Command introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 13.2X50-D10 (ELS).
Command introduced in Junos OS Release 15.1X49-D70 for SRX Series devices.

Description

Display Multiple VLAN Registration Protocol (MVRP) statistics in the form of Multiple Registration Protocol data unit (MRPDU) messages.

Options

```
none—Show MVRP statistics for all interfaces on the switch.
interface interface-name—(Optional) Show MVRP statistics for the specified interface.
```

Required Privilege Level

```
view
```

Related Documentation

- show mvrp on page 2136
- clear mvrp statistics
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches
- Verifying That MVRP Is Working Correctly on Switches
- Verifying That MVRP Is Working Correctly on EX Series Switches with ELS Support

List of Sample Output

```
show mvrp statistics interface xe-0/1/1.0 on page 2151
show mvrp statistics on page 2151
show mvrp statistics (SRX Devices) on page 2151
```

Output Fields

```
Table 146 on page 2142 lists the output fields for the show mvrp statistics command on EX Series switches. Output fields are listed in the approximate order in which they appear.
```
### Table 149: show mvrp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MRPU received</td>
<td>Number of MRPU messages received on the switch.</td>
</tr>
<tr>
<td>Invalid PDU received</td>
<td>Number of invalid MRPU messages received on the switch.</td>
</tr>
<tr>
<td>New received</td>
<td>Number of new messages received on the switch.</td>
</tr>
<tr>
<td>Join Empty received</td>
<td>Number of MRPU JoinEmpty messages received on the switch. Either this value or the value for JoinIn received should increase when the value for MRPU received increases. If this value is not incrementing when it should, you might have a Junos OS release version compatibility issue. To fix a version compatibility issue, see Configuring Multiple VLAN Registration Protocol (MVRP) on Switches.</td>
</tr>
<tr>
<td>Join In received</td>
<td>Number of MRPU JoinIn messages received on the switch. Either this value or the value for JoinEmpty received should increase when the value for MRPU received increases. If this value is not incrementing when it should, you might have a Junos OS release version compatibility issue. To fix a version compatibility issue, see Configuring Multiple VLAN Registration Protocol (MVRP) on Switches.</td>
</tr>
<tr>
<td>Empty received</td>
<td>Number of MRPU Empty messages received on the switch.</td>
</tr>
<tr>
<td>In received</td>
<td>Number of MRPU In messages received on the switch.</td>
</tr>
<tr>
<td>Leave received</td>
<td>Number of MRPU Leave messages received on the switch.</td>
</tr>
<tr>
<td>LeaveAll received</td>
<td>Number of LeaveAll messages received on the switch.</td>
</tr>
<tr>
<td>MRPU transmitted</td>
<td>Number of MRPU messages transmitted from the switch.</td>
</tr>
<tr>
<td>MRPU transmit failures</td>
<td>Number of MRPU transmit failures from the switch.</td>
</tr>
<tr>
<td>New transmitted</td>
<td>Number of new messages transmitted from the switch.</td>
</tr>
<tr>
<td>Join Empty transmitted</td>
<td>Number of JoinEmpty messages sent from the switch.</td>
</tr>
<tr>
<td>Join In transmitted</td>
<td>Number of MRPU JoinIn messages sent from the switch.</td>
</tr>
<tr>
<td>Empty transmitted</td>
<td>Number of MRPU Empty messages sent from the switch.</td>
</tr>
<tr>
<td>In transmitted</td>
<td>Number of MRPU In messages sent from the switch.</td>
</tr>
<tr>
<td>Leave transmitted</td>
<td>Number of MRPU Leave Empty messages sent from the switch.</td>
</tr>
<tr>
<td>LeaveAll transmitted</td>
<td>Number of MRPU LeaveAll messages sent from the switch.</td>
</tr>
</tbody>
</table>

Table 150 on page 2150 lists the output fields for the show mvrp statistics command on SRX devices. Output fields are listed in the approximate order in which they appear.
### Table 150: show mvrp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Interface for which MVRP statistics are displayed.</td>
</tr>
<tr>
<td>VLAN IDs registered</td>
<td>Number of Virtual LAN (VLAN) IDs registered.</td>
</tr>
<tr>
<td>Sent MVRP PDUs</td>
<td>Number of MRPDU messages transmitted from the switch.</td>
</tr>
<tr>
<td>Received MVRP PDUs without error</td>
<td>Number of MRPDU messages received on the switch.</td>
</tr>
<tr>
<td>Received MVRP PDUs with error</td>
<td>Number of invalid MRPDU messages received on the switch.</td>
</tr>
<tr>
<td>Transmitted Join Empty</td>
<td>Number of JoinEmpty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted Leave All</td>
<td>Number of MRP LeaveAll messages sent from the switch.</td>
</tr>
<tr>
<td>Received Join In</td>
<td>Number of MRP JoinIn messages received on the switch. Either this value or the value for Received Join Empty should increase when the value for Received MVRP PDUs without error increases. If this value is not incrementing when it should, you might have a Junos OS release compatibility issue. To resolve the issue, see Configuring Multiple VLAN Registration Protocol (MVRP) on Switches.</td>
</tr>
<tr>
<td>Transmitted Join In</td>
<td>Number of MRP JoinIn messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted Empty</td>
<td>Number of MRP Empty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted Leave</td>
<td>Number of MRP LeaveEmpty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted In</td>
<td>Number of MRP In messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted New</td>
<td>Number of New messages transmitted from the switch.</td>
</tr>
<tr>
<td>Received Leave All</td>
<td>Number of LeaveAll messages received on the switch.</td>
</tr>
<tr>
<td>Received Leave</td>
<td>Number of MRP Leave messages received on the switch.</td>
</tr>
<tr>
<td>Received In</td>
<td>Number of MRP In messages received on the switch.</td>
</tr>
<tr>
<td>Received Empty</td>
<td>Number of MRP Empty messages received on the switch.</td>
</tr>
<tr>
<td>Received Join Empty</td>
<td>Number of MRP JoinEmpty messages received on the switch. Either this value or the value for Received Join In should increase when the value for Received MVRP PDUs without error increases. If this value is not incrementing when it should, you might have a Junos OS release compatibility issue. To resolve the issue, see Configuring Multiple VLAN Registration Protocol (MVRP) on Switches.</td>
</tr>
<tr>
<td>Received New</td>
<td>Number of New messages received on the switch.</td>
</tr>
</tbody>
</table>
### Sample Output

**show mvrp statistics interface xe-0/1/1.0**

```
user@switch> show mvrp statistics interface xe-0/1/1.0

MVRP statistics
MRPDU received                : 3342
Invalid PDU received          : 0
New received                  : 2
Join Empty received           : 1116
Join In received              : 2219
Empty received                : 2
In received                   : 2
Leave received                : 1
LeaveAll received             : 1117
MRPDU transmitted             : 3280
MRPDU transmit failures       : 0
New transmitted               : 0
Join Empty transmitted        : 1114
Join In transmitted           : 2163
Empty transmitted             : 1
In transmitted                : 1
Leave transmitted             : 1
LeaveAll transmitted          : 1111
```

**show mvrp statistics**

```
user@host> show mvrp statistics

MVRP statistics for routing instance 'default-switch'
Interface name                  : xe-0/1/1
VLAN IDs registered             : 117
Sent MVRP PDUs                  : 118824
Received MVRP PDUs without error: 118848
Received MVRP PDUs with error   : 0
Transmitted Join Empty          : 5229
Transmitted Leave All           : 2
Received Join In                : 11884924
Transmitted Join In             : 1835
Transmitted Empty               : 93606408
Transmitted Leave               : 888
Transmitted New                 : 13780024
Transmitted New                 : 2692
Received Leave All              : 118761
Received Leave                  : 97
Received In                     : 3869
Received Empty                  : 828
Received Join Empty             : 2020152
Received New                    : 224
...
```

**show mvrp statistics (SRX Devices)**

```
user@host> show mvrp statistics
```
MVRP statistics for routing instance 'default-switch'

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>ge-0/0/1</td>
</tr>
<tr>
<td>VLAN IDs registered</td>
<td>2</td>
</tr>
<tr>
<td>Sent MVRP PDUs</td>
<td>41</td>
</tr>
<tr>
<td>Received MVRP PDUs without error</td>
<td>28</td>
</tr>
<tr>
<td>Received MVRP PDUs with error</td>
<td>0</td>
</tr>
<tr>
<td>Transmitted Join Empty</td>
<td>0</td>
</tr>
<tr>
<td>Transmitted Leave All</td>
<td>20</td>
</tr>
<tr>
<td>Received Join In</td>
<td>0</td>
</tr>
<tr>
<td>Transmitted Join In</td>
<td>0</td>
</tr>
<tr>
<td>Transmitted Empty</td>
<td>114</td>
</tr>
<tr>
<td>Transmitted Leave</td>
<td>10</td>
</tr>
<tr>
<td>Transmitted In</td>
<td>10</td>
</tr>
<tr>
<td>Transmitted New</td>
<td>0</td>
</tr>
<tr>
<td>Received Leave All</td>
<td>1</td>
</tr>
<tr>
<td>Received Leave</td>
<td>0</td>
</tr>
<tr>
<td>Received In</td>
<td>0</td>
</tr>
<tr>
<td>Received Empty</td>
<td>67</td>
</tr>
<tr>
<td>Received Join Empty</td>
<td>24</td>
</tr>
<tr>
<td>Received New</td>
<td>0</td>
</tr>
</tbody>
</table>
CHAPTER 24

OSPF Operational Commands

- clear (ospf | ospf3) database
- clear (ospf | ospf3) io-statistics
- clear (ospf | ospf3) neighbor
- clear (ospf | ospf3) overload
- clear (ospf | ospf3) statistics
- show (ospf | ospf3) backup coverage
- show (ospf | ospf3) backup lsp
- show (ospf | ospf3) backup neighbor
- show (ospf | ospf3) backup spf
- show ospf context-identifier
- show ospf database
- show ospf3 database
- show (ospf | ospf3) interface
- show (ospf | ospf3) io-statistics
- show (ospf | ospf3) log
- show (ospf | ospf3) neighbor
- show (ospf | ospf3) overview
- show (ospf | ospf3) route
- show (ospf | ospf3) statistics
clear (ospf | ospf3) database

List of Syntax  Syntax on page 2154
Syntax (EX Series Switch and QFX Series) on page 2154

Syntax  clear (ospf | ospf3) database
<all>
<advertising-router (router-id | self)>
<area area-id>
<asbrsummary>
<external>
<instance instance-name>
<interarea-prefix>
<interarea-router>
<interarea-prefix>
<link-local>
<logical-system (all | logical-system-name)>
<lsa-id lsa-id>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>

Syntax (EX Series Switch and QFX Series)  clear (ospf | ospf3) database
<all>
<advertising-router (router-id | self)>
<area area-id>
<asbrsummary>
<external>
<instance instance-name>
<interarea-prefix>
<interarea-router>
<interarea-prefix>
<link-local>
<lsa-id lsa-id>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<router>

Release Information  Command introduced before Junos OS Release 7.4.
advertising-router router-id, netsummary, network, nssa, opaque-area, and router options added in Junos OS Release 8.3. You must use the purge command with these options.
area area-id option added in Junos OS Release 8.3.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option added in Junos OS Release 9.2.

advertising-router (router-id | self) option added in Junos OS Release 9.5.

advertising-router (router-id | self) option introduced in Junos OS Release 9.5 for EX Series switches.

Command introduced in Junos OS Release 11.3 for the QFX Series.

Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

purge option (and all options that are dependent on the purge option) hidden in Junos OS Release 13.3.

Description

With the master Routing Engine, delete entries in the Open Shortest Path First (OSPF) link-state advertisement (LSA) database. With the backup Routing Engine, delete the OSPF LSA database and sync the new database with the master Routing Engine.

---

**CAUTION:** You can also use the purge command with any of the options to discard rather than delete the specified LSA entries. This command is useful only for testing. Use it with care, because it causes significant network disruption.

---

Options

- **all**—Delete all LSAs other than the system's own LSAs, which are regenerated. To resynchronize the database, the system destroys all adjacent neighbors that are in the state EXSTART or higher. The neighbors are then reacquired and the databases are synchronized.

- **advertising-router (router-id | self)**—(Optional) Discard entries for the LSA entries advertised by the specified routing device or by this routing device.

- **area area-id**—(Optional) Discard entries for the LSAs in the specified area.

- **asbrsummary**—(Optional) Discard summary AS boundary router LSA entries.

- **external**—(Optional) Discard external LSAs.

- **instance instance-name**—(Optional) Delete or discard entries for the specified routing instance only.

- **inter-area-prefix**—(OSPFv3 only) (Optional) Discard interarea prefix LSAs.

- **inter-area-router**—(OSPFv3 only) (Optional) Discard interarea router LSAs.

- **intra-area-prefix**—(OSPFv3 only) (Optional) Discard intra-area prefix LSAs.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

- **link-local**—(Optional) Delete link-local LSAs.

- **lsa-id lsa-id**—(Optional) Discard the LSA entries with the specified LSA identifier.

- **netsummary**—(Optional) Discard summary network LSAs.
network—(Optional) Discard network LSAs.

nssa—(Optional) Discard not-so-stubby area (NSSA) LSAs.

opaque-area—(Optional) Discard opaque area-scope LSAs.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional)
  Delete the entries for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

router—(Optional) Discard router LSAs.

purge—(Optional) Discard all entries in the link-state advertisement database. All link-state advertisements are set to MAXAGE and are flooded. The database is repopulated when the originators of the link-state advertisements receive the MAXAGE link-state advertisements and reissue them.

Required Privilege Level clear

Related Documentation
  • show ospf database on page 2180
  • show ospf3 database on page 2191

List of Sample Output clear ospf database all on page 2156

Output Fields
  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf database all

  user@host> clear ospf database all
clear (ospf | ospf3) io-statistics

List of Syntax  Syntax on page 2157
Syntax (EX Series Switch and QFX Series) on page 2157

Syntax  clear (ospf | ospf3) io-statistics
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and QFX Series)  clear (ospf | ospf3) io-statistics

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Clear Open Shortest Path First (OSPF) input and output statistics.

Options  none—Clear OSPF input and output statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege  clear

Level

List of Sample Output  clear ospf io-statistics on page 2157

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf io-statistics

user@host> clear ospf io-statistics
**clear (ospf | ospf3) neighbor**

**List of Syntax**

Syntax on page 2158  
Syntax (EX Series Switch and QFX Series) on page 2158

**Syntax**

```
clear (ospf | ospf3) neighbor
<all>
<area area-id>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
<neighbor>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

**Syntax (EX Series Switch and QFX Series)**

```
clear (ospf | ospf3) neighbor
<all>
<area area-id>
<instance instance-name>
<interface interface-name>
<neighbor>
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
**realm** option introduced in Junos OS Release 9.2.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Tear down Open Shortest Path First (OSPF) neighbor connections.

**Options**

- **all**—Tear down OSPF connections with all neighbors for all routing instances.
  - **area area-id**—(Optional) Tear down neighbor connections for the specified area only.
  - **instance instance-name**—(Optional) Tear down neighbor connections for the specified routing instance only.
  - **interface interface-name**—(Optional) Tear down neighbor connections for the specified interface only.
  - **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
  - **neighbor**—(Optional) Clear the state of the specified neighbor only.
  - **realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(Optional) (OSPFv3 only) Clear the state of the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.
Required Privilege Level  clear

Related Documentation  •  show (ospf | ospf3) neighbor on page 2213

List of Sample Output  clear ospf neighbor all on page 2159

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf neighbor all

user@host>  clear ospf neighbor all
clear (ospf | ospf3) overload

List of Syntax
Syntax on page 2160
Syntax (EX Series Switches) on page 2160

Syntax clear (ospf | ospf3) overload
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches) clear (ospf | ospf3) overload
<instance instance-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Clear the Open Shortest Path First (OSPF) overload bit and rebuild link-state advertisements (LSAs).

Options
none—Clear the overload bit and rebuild LSAs for all routing instances.

instance instance-name—(Optional) Clear the overload bit and rebuild LSAs for the specified routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
Level clear

List of Sample Output clear ospf overload on page 2160

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ospf overload

user@host> clear ospf overload
clear (ospf | ospf3) statistics

List of Syntax Syntax on page 2161
Syntax (EX Series Switch and QFX Series) on page 2161

Syntax clear (ospf | ospf3) statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switch and QFX Series) clear (ospf | ospf3) statistics
<instance instance-name>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Clear Open Shortest Path First (OSPF) statistics.

Options none—Clear OSPF statistics.
instance instance-name—(Optional) Clear statistics for the specified routing instance only.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Clear statistics for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege clear

Level

Related Documentation • show (ospf | ospf3) statistics on page 2233

List of Sample Output clear ospf statistics on page 2162

Output Fields See show (ospf | ospf3) statistics for an explanation of output fields.
Sample Output

clear ospf statistics

The following sample output displays OSPF statistics before and after the clear ospf statistics command is entered:

```
user@host> show ospf statistics

Packet type     Total                  Last 5 seconds
               Sent      Received        Sent      Received
Hello           3254          2268           3             1
DbD             41            46           0             0
LSReq           8             7           0             0
LSUpdate        212           154           0             0
LSAck           65            98           0             0

DBDs retransmitted :                     3, last 5 seconds :          0
LSAs flooded :                             12, last 5 seconds :          0
LSAs flooded high-prio :                  0, last 5 seconds :          0
LSAs retransmitted :                      0, last 5 seconds :          0
LSAs transmitted to nbr:                  3, last 5 seconds :          0
LSAs requested :                          5, last 5 seconds :          0
LSAs acknowledged :                       19, last 5 seconds :          0

Flood queue depth :                       0
Total rexmit entries :                    0
db summaries :                            0
lsreq entries :                           0

Receive errors:
   626 subnet mismatches

user@host> clear ospf statistics

user@host> show ospf statistics

Packet type     Total                  Last 5 seconds
               Sent      Received        Sent      Received
Hello           3             1           3             1
DbD             0             0           0             0
LSReq           0             0           0             0
LSUpdate        0             0           0             0
LSAck           0             0           0             0

DBDs retransmitted :                     0, last 5 seconds :          0
LSAs flooded :                             0, last 5 seconds :          0
LSAs flooded high-prio :                  0, last 5 seconds :          0
LSAs retransmitted :                      0, last 5 seconds :          0
LSAs transmitted to nbr:                  0, last 5 seconds :          0
LSAs requested :                          0, last 5 seconds :          0
LSAs acknowledged :                       0, last 5 seconds :          0

Flood queue depth :                       0
Total rexmit entries :                    0
db summaries :                            0
lsreq entries :                           0
```
Receive errors:
  None
show (ospf | ospf3) backup coverage

Syntax

show (ospf | ospf3) backup coverage
<instance instance-name>
<logical-system (all | logical-system-name)>
realm (ipv4-unicast | ipv46-unicast>
<topology topology-name>

Syntax (QFX Series)

show (ospf | ospf3) backup coverage
<instance instance-name>
<topology topology-name>

Release Information

Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about the level of backup coverage available for all the nodes and prefixes in the network.

Options

none—Display information about the level backup coverage for all OSPF routing instances in all logical systems.

logical-system (all | logical-system-name)—(Optional) Display information about the level of backup coverage for all logical systems or for a specific logical system.

instance instance-name—(Optional) Display information about the level of backup coverage for a specific OSPF routing instance.

realm (ipv4-unicast | ipv6-unicast)—(Optional) (OSPFv3 only) Display information about the level of backup coverage for the specific OSPFv3 realm, or address family.

topology (default | topology-name)—(Optional) (OSPFv2 only) Display information about the level of backup coverage for the specific OSPF topology.

Required Privilege Level

view

Related Documentation

• show (ospf | ospf3) backup lsp on page 2167

List of Sample Output

show ospf backup coverage on page 2165
show ospf3 backup coverage on page 2165

Output Fields

Table 151 on page 2165 lists the output fields for the show (ospf | ospf3) backup coverage command. Output fields are listed in the approximate order in which they appear.
Table 151: show (ospf | ospf3) backup coverage Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Coverage</td>
<td>Information about backup coverage for each OSPF node.</td>
</tr>
<tr>
<td>Area</td>
<td>Area number. Area 0.0.0.0 is the backbone.</td>
</tr>
<tr>
<td>Covered Nodes</td>
<td>Number of nodes for which backup coverage is available.</td>
</tr>
<tr>
<td>Total Nodes</td>
<td>Total number of OSPF nodes.</td>
</tr>
<tr>
<td>Route Coverage</td>
<td>Information about backup coverage for each type of OSPF route.</td>
</tr>
<tr>
<td>Path Type</td>
<td>Type of OSPF path: Intra, Inter, Ext1, Ext2, and All.</td>
</tr>
<tr>
<td>Covered Routes</td>
<td>For each path type, the number of routes for which backup coverage is available.</td>
</tr>
<tr>
<td>Total Routes</td>
<td>For each path type, the total number of configured routes.</td>
</tr>
<tr>
<td>Percent Covered</td>
<td>For all nodes and for each path type, the percentage for which backup coverage is available.</td>
</tr>
</tbody>
</table>

Sample Output

show ospf backup coverage

user@host> show ospf backup coverage
Topology default coverage:

Node Coverage:

<table>
<thead>
<tr>
<th>Area</th>
<th>Covered Nodes</th>
<th>Total Nodes</th>
<th>Percent Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>4</td>
<td>5</td>
<td>80.00%</td>
</tr>
</tbody>
</table>

Route Coverage:

<table>
<thead>
<tr>
<th>Path Type</th>
<th>Covered Routes</th>
<th>Total Routes</th>
<th>Percent Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra</td>
<td>8</td>
<td>14</td>
<td>57.14%</td>
</tr>
<tr>
<td>Inter</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
</tr>
<tr>
<td>Ext1</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
</tr>
<tr>
<td>Ext2</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
</tr>
<tr>
<td>All</td>
<td>9</td>
<td>15</td>
<td>60.00%</td>
</tr>
</tbody>
</table>

show ospf3 backup coverage

user @host > show ospf3 backup coverage
show ospf3 backup coverage
Node Coverage:
<table>
<thead>
<tr>
<th>Area</th>
<th>Covered Nodes</th>
<th>Total Nodes</th>
<th>Percent Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>4</td>
<td>5</td>
<td>80.00%</td>
</tr>
</tbody>
</table>

**Route Coverage:**

<table>
<thead>
<tr>
<th>Path Type</th>
<th>Covered Routes</th>
<th>Total Routes</th>
<th>Percent Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra</td>
<td>4</td>
<td>6</td>
<td>66.67%</td>
</tr>
<tr>
<td>Inter</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
</tr>
<tr>
<td>Ext1</td>
<td>0</td>
<td>0</td>
<td>100.00%</td>
</tr>
<tr>
<td>Ext2</td>
<td>1</td>
<td>1</td>
<td>100.00%</td>
</tr>
<tr>
<td>All</td>
<td>5</td>
<td>7</td>
<td>71.43%</td>
</tr>
</tbody>
</table>
show (ospf | ospf3) backup lsp

Syntax
```
show (ospf | ospf3) backup lsp
  <logical-system (all | logical-system-name)>
  <realm (ipv4-unicast | ipv6-unicast)>
```

Release Information
Command introduced in Junos OS Release 10.0.

Description
Display information about MPLS label-switched-paths (LSPs) designated as backup routes for OSPF routes.

**NOTE:** MPLS LSPs can be used as backup routes only for routes in the default OSPFV2 topology and not for any configured topology. Additionally, MPLS LSPs cannot be used as backup routes for nondefault instances either for OSPFV2 or OSPFV3.

Options
- none—Display information all MPLS LSPs designated as backup routes.
- `logical-system (all | logical-system-name)`—(Optional) Display information about MPLS LSPs designated as backup routes for all logical systems or a specific logical system.
- `realm (ipv4-unicast | ipv6-unicast)`—(Optional) (OSPFv3 only) Display information about MPLS LSPs designated as backup routes for a specific realm, or address family.

Required Privilege
view

Related Documentation
- show (ospf | ospf3) backup coverage on page 2164

List of Sample Output
- show ospf backup lsp on page 2168
- show ospf3 backup lsp on page 2168

Output Fields
Table 152 on page 2167 lists the output fields for the `show (ospf | ospf3) backup lsp` command. Output fields are listed in the approximate order in which they appear.

**Table 152: show (ospf | ospf3) backup lsp Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS LSP name</td>
<td>Name of each MPLS LSP designated as a backup path.</td>
</tr>
<tr>
<td>Egress</td>
<td>IP address of the egress router for the LSP.</td>
</tr>
</tbody>
</table>
Table 152: show (ospf | ospf3) backup lsp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>State of the LSP:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Up</strong>—The router can detect RSVP hello messages from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—The router has received one of the following indications:</td>
</tr>
<tr>
<td></td>
<td>• Communication failure from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Communication from IGP that the neighbor is unavailable.</td>
</tr>
<tr>
<td></td>
<td>• Change in the sequence numbers in the RSVP hello messages sent by the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deleted</strong>—The LSP is no longer available as a backup path.</td>
</tr>
<tr>
<td>Last change</td>
<td>Time elapsed since the neighbor state changed either from <strong>up</strong> or <strong>down</strong> or from <strong>down</strong> to <strong>up</strong>. The format is <strong>hh:mm:ss</strong>.</td>
</tr>
<tr>
<td>TE-metric</td>
<td>Configured traffic engineering metric.</td>
</tr>
<tr>
<td>Metric</td>
<td>Configured metric.</td>
</tr>
</tbody>
</table>

Sample Output

show ospf backup lsp

```
user@host> show ospf backup lsp
tobanff
Egress: 10.255.71.239, Status: up, Last change: 00:00:23
TE-metric: 0, Metric: 0
```

Sample Output

show ospf3 backup lsp

```
user@host> show ospf3 backup lsp
tobanff
Egress: 10.255.71.239, Status: up, Last change: 00:00:45
TE-metric: 0, Metric: 0
```
show (ospf | ospf3) backup neighbor

Syntax
show (ospf | ospf3) backup neighbor
<area area-id>
<instance (default | instance-name)>
<logical-system (default | ipv4-multicast | logical-system-name)>
<topology (default | ipv4-multicast | topology-name)>

Syntax (QFX Series)
show (ospf | ospf3) backup neighbor
<area area-id>
<instance instance-name>
<topology (default | ipv4-multicast | topology-name)>

Release Information
Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Display the neighbors through which direct next hops for the backup paths are available.

Options
none—Display all neighbors that have direct next hops for backup paths.
area area-id—(Optional) Display the area information.
instance (default | instance-name)—(Optional) Display information about the default routing instance or a particular routing instance.
logical-system (default | ipv4-multicast | logical-system-name)—(Optional) Display information about the default logical system, IPv4 multicast logical system, or a particular logical system.
topology (default | ipv4-multicast | topology-name)—(OSPFv2 only) (Optional) Display information about the default topology, IPv4 multicast topology, or a particular topology.

Required Privilege
view

Related Documentation
• show (ospf | ospf3) backup spf on page 2171

List of Sample Output
show ospf backup neighbor on page 2170

Output Fields
Table 153 on page 2170 lists the output fields for the show (ospf | ospf3) backup neighbor command. Output fields are listed in the approximate order in which they appear.
### Table 153: show (ospf | ospf3) backup neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor to Self Metric</td>
<td>Metric from the backup neighbor to the OSPF node.</td>
<td>All levels</td>
</tr>
<tr>
<td>Self to Neighbor Metric</td>
<td>Metric from the OSPF node to the backup neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Direct next-hop</td>
<td>Interface and address of the direct next hop.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

### Sample Output

**show ospf backup neighbor**

```
user@host> show ospf backup neighbor
Topology default backup neighbors:

Area 0.0.0.5 backup neighbors:

10.0.0.5
Neighbor to Self Metric: 5
Self to Neighbor Metric: 5
Direct next-hop: ge-4/0/0.111 via 10.0.175.5

10.0.0.6
Neighbor to Self Metric: 5
Self to Neighbor Metric: 5
Direct next-hop: ge-4/1/0.110 via 10.0.176.6
```
show (ospf | ospf3) backup spf

Syntax

show (ospf | ospf3) backup spf
  <brief | detail>
  <area area-id>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <no-coverage>
  <node-id>
  <realm (ipv4–unicast | ipv6–unicast)>
  <topology (default | ipv4-mcast | topology-name)>

Syntax (QFX Series)

show (ospf | ospf3) backup spf
  <brief | detail>
  <area area-id>
  <instance instance-name>
  <no-coverage>
  <node-id>
  <topology (default | ipv4-mcast | topology-name)>

Release Information

Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display information about OSPF shortest-path-first calculations for backup paths.

Options

none—Display information about OSPF shortest-path-first (SPF) calculations for all
backup paths for all destination nodes.

brief | detail—(Optional) Display the specified level of output.

area area-id—(Optional) Display the area information.

instance instance-name—(Optional) Display information about the routing instance.

logical-system (all | logical-system-name)—(Optional) Display information about all
logical systems or a specific logical system.

no-coverage—(Optional) Display information if there is no backup coverage.

node-id—(Optional) Display information about the node specified.

realm (ipv4–unicast | ipv6–unicast)—(Optional) Display information about the ipv4 or
ipv6 realm.

topology (default | ipv4-mcast | topology-name)—(Optional) (OSPFv2 only) Display
information about the default topology, IPv4 multicast topology, or a specific topology.

Required Privilege

view
Sample Output

```
show ospf backup spf

user@host> show ospf backup spf

Topology default results:

Area 0.0.0.0 results:

pro16-d-lo0.xxx.yyyy.net
  Self to Destination Metric: 1
  Parent Node: pro16-b-lo0.xxx.yyyy.net
  Primary next-hop: at-1/0/1.0
  Backup Neighbor: pro16-c-lo0.xxx.yyyy.net (LSP endpoint)
    Neighbor to Destination Metric: 4, Neighbor to Self Metric: 3
    Self to Neighbor Metric: 3
    Not eligible, Reason: Path loops
  Backup Neighbor: pro16-d-lo0.xxx.yyyy.net
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
```
show ospf backup spf detail

user@host> show ospf backup spf detail

Topology default results:

Area 0.0.0.0 results:

11.14.10.2
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: ae0.0
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.52
  Self to Destination Metric: 1
  Parent Node: 11.14.10.2
  Primary next-hop: ae0.0 via 11.14.10.2
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops

10.255.71.242
  Self to Destination Metric: 1
  Parent Node: 10.255.70.103
  Primary next-hop: as0.0
  Backup Neighbor: 10.255.71.242
    Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
    Not eligible, Reason: Primary next-hop link fate sharing
  Backup Neighbor: 10.255.71.243
    Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
    Self to Neighbor Metric: 1
    Not eligible, Reason: Path loops
  Backup Neighbor: 10.255.71.52
    Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
    Self to Neighbor Metric: 1
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Self to Destination Metric</th>
<th>Parent Node</th>
<th>Primary next-hop</th>
<th>Backup Neighbor</th>
<th>Neighbor to Destination Metric</th>
<th>Neighbor to Self Metric</th>
<th>Self to Neighbor Metric</th>
<th>Eligibility</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.71.243</td>
<td>1</td>
<td>10.255.70.103</td>
<td>so-6/0/0.0</td>
<td>10.255.71.243</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>Not eligible</td>
<td>Path loops</td>
</tr>
<tr>
<td>10.255.71.52</td>
<td>16</td>
<td>10.255.71.243</td>
<td>10.255.71.52</td>
<td>10.255.71.243</td>
<td>16</td>
<td>15</td>
<td>1</td>
<td>Not eligible</td>
<td>Path loops</td>
</tr>
<tr>
<td>10.255.71.242</td>
<td>17</td>
<td>10.255.71.243</td>
<td>10.255.71.242</td>
<td>10.255.71.242</td>
<td>17</td>
<td>15</td>
<td>1</td>
<td>Not evaluated</td>
<td>Interface is already covered</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Self to Destination Metric</th>
<th>Parent Node</th>
<th>Primary next-hop</th>
<th>Backup Neighbor</th>
<th>Neighbor to Destination Metric</th>
<th>Neighbor to Self Metric</th>
<th>Self to Neighbor Metric</th>
<th>Eligibility</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.15.0.1</td>
<td>2</td>
<td>10.255.71.243</td>
<td>ae0.0 via 11.14.10.2</td>
<td>10.255.71.243</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Not eligible</td>
<td>Primary next-hop link fate sharing</td>
</tr>
<tr>
<td>10.255.71.242</td>
<td>15</td>
<td>10.255.71.243</td>
<td>10.255.71.242</td>
<td>10.255.71.242</td>
<td>17</td>
<td>15</td>
<td>1</td>
<td>Eligible</td>
<td>Contributes backup next-hop</td>
</tr>
<tr>
<td>10.255.71.238</td>
<td>2</td>
<td>10.255.71.243</td>
<td>as0.0</td>
<td>10.255.71.243</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Not eligible</td>
<td>Primary next-hop link fate sharing</td>
</tr>
<tr>
<td>10.255.71.239</td>
<td>2</td>
<td>12.15.0.1</td>
<td>so-6/0/0.0</td>
<td>10.255.71.238</td>
<td>15</td>
<td>15</td>
<td>1</td>
<td>Eligible</td>
<td>Contributes backup next-hop</td>
</tr>
</tbody>
</table>
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered

14.15.0.2
Self to Destination Metric: 3
Parent Node: 10.255.71.239
Primary next-hop: so-6/0/0.0
Backup next-hop: ae0.0 via 11.14.10.2
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered

show ospf3 backup spf

user@host> show ospf3 backup spf

Area 0.0.0.0 results:

10.255.71.52;0.0.0.5
Self to Destination Metric: 1
Parent Node: 10.255.70.103
Primary next-hop: ae0.0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops

10.255.71.52
Self to Destination Metric: 1
Parent Node: 10.255.71.52;0.0.0.5
Primary next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops

10.255.71.242
Self to Destination Metric: 1
Parent Node: 10.255.70.103
Primary next-hop: as0.0
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 2, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops

10.255.71.243
Self to Destination Metric: 1
Parent Node: 10.255.70.103
Primary next-hop: so-6/0/0.0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 0, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not eligible, Reason: Path loops

10.255.71.243;0.0.0.2
Self to Destination Metric: 2
Parent Node: 10.255.71.243
Primary next-hop: so-6/0/0.0
Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered

10.255.71.238
Self to Destination Metric: 2
Parent Node: 10.255.71.243
Primary next-hop: so-6/0/0.0
Backup next-hop: as0.0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered

10.255.71.239
Self to Destination Metric: 2
Parent Node: 10.255.71.239:0.0.0.2
Primary next-hop: so-6/0/0.0
Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 1, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 16, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered

10.255.71.239:0.0.0.4
Self to Destination Metric: 3
Parent Node: 10.255.71.239
Primary next-hop: so-6/0/0.0
Backup next-hop: ae0.0 via fe80::290:69ff:fe0f:67f0
Backup Neighbor: 10.255.71.243
Neighbor to Destination Metric: 2, Neighbor to Self Metric: 1
Self to Neighbor Metric: 1
Not eligible, Reason: Primary next-hop link fate sharing
Backup Neighbor: 10.255.71.52
Neighbor to Destination Metric: 15, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Eligible, Reason: Contributes backup next-hop
Backup Neighbor: 10.255.71.242
Neighbor to Destination Metric: 17, Neighbor to Self Metric: 15
Self to Neighbor Metric: 1
Not evaluated, Reason: Interface is already covered
# show ospf context-identifier

## List of Syntax

Syntax on page 2178
Syntax (EX Series Switches and QFX Series) on page 2178

```markdown
**Syntax**

`show ospf context-identifier`

- `<brief | detail>`
- `<area area-id>`
- `<context-id>`
- `<instance instance-name>`
- `<logical-system (all | logical-system-name)>`
```

## Syntax (EX Series Switches and QFX Series)

```markdown
**Syntax**

`show ospf context-identifier`

- `<brief | detail>`
- `<area area-id>`
- `<context-id>`
- `<instance instance-name>`
```

## Release Information

Command introduced in Junos OS Release 10.4.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

## Description

Display the context identifier information processed and advertised by Open Shortest Path First (OSPF) for egress protection.

## Options

- **none**—Display information about all context identifiers.
- **brief | detail**—(Optional) Display the specified level of output.
- **area area-id**—(Optional) Display information about the context identifier for the specified area.
- **context-id**—(Optional) Display information about the specified context identifier.
- **instance instance-name**—(Optional) Display information about the context identifier for the specified routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

## Required Privilege

View

## Related Documentation

- `egress-protection (Layer 2 circuit)` in the Junos OS VPNs Library for Routing Devices
- `egress-protection (MPLS)` in the Junos OS VPNs Library for Routing Devices
List of Sample Output  show ospf context-identifier on page 2179
show ospf context-identifier detail on page 2179

Output Fields  Table 155 on page 2179 lists the output fields for the show ospf context-identifier command. Output fields are listed in the approximate order in which they appear.

Table 155: show ospf context-identifier Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>IPv4 address that defines a protection pair. The context is manually configured on both primary and protector provider edge (PE) devices.</td>
<td>All levels</td>
</tr>
<tr>
<td>Status</td>
<td>State of the path: active or inactive.</td>
<td>All levels</td>
</tr>
<tr>
<td>Metric</td>
<td>Advertised OSPF metric.</td>
<td>All levels</td>
</tr>
<tr>
<td>Area</td>
<td>OSPF area number.</td>
<td>All levels</td>
</tr>
<tr>
<td>Other</td>
<td>Other advertisements received by the OSPF node:</td>
<td>detail</td>
</tr>
<tr>
<td>Advertisements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertising router</td>
<td>Address of the device that sent the advertisement.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of OSPF path: inter-area and stub.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Advertised OSPF metric.</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>No additional advertisements were received by the OSPF node.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show ospf context-identifier

```
user@host> show ospf context-identifier

  Context-id: 2.2.4.3
    Status: active, Metric: 65534, PE role: protector, Area: 0.0.0.0
```

show ospf context-identifier detail

```
user@host> show ospf context-identifier detail

  Context-id: 88.24.13.1
    Status: inactive, Metric: 0, PE role: protector, Area: 0.0.0.13
    Other Advertisements:
      Advertising router: 8.8.8.103
      Type: stub link
      Metric: 65534
```
**show ospf database**

<table>
<thead>
<tr>
<th>List of Syntax</th>
<th>Syntax on page 2180</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>Syntax (EX Series Switches and QFX Series) on page 2180</td>
</tr>
</tbody>
</table>

**Syntax**

show ospf database

- `<brief | detail | extensive | summary>`
- `<advertising-router (address | self)>`
- `<area area-id>`
- `<asbrsummary>`
- `<external>`
- `<instance instance-name>`
- `<link-local>`
- `<logical-system (all | logical-system-name)>`
- `<lsa-id lsa-id>`
- `<netsummary>`
- `<network>`
- `<nssa>`
- `<opaque-area>`
- `<router>`

**Syntax (EX Series Switches and QFX Series)**

show ospf database

- `<brief | detail | extensive | summary>`
- `<advertising-router (address | self)>`
- `<area area-id>`
- `<asbrsummary>`
- `<external>`
- `<instance instance-name>`
- `<link-local>`
- `<logical-system (all | logical-system-name)>`
- `<lsa-id lsa-id>`
- `<netsummary>`
- `<network>`
- `<nssa>`
- `<opaque-area>`
- `<router>`

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `advertising-router self (address | self)` option introduced in Junos OS Release 9.5.
- `advertising-router self (address | self)` option introduced in Junos OS Release 9.5 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display the entries in the OSPF version 2 (OSPFv2) link-state database, which contains data about link-state advertisement (LSA) packets.

**Options**

- `none`—Display standard information about entries in the OSPFv2 link-state database for all routing instances.
brief | detail | extensive | summary—(Optional) Display the specified level of output.

advertising-router (address | self)—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.

area area-id—(Optional) Display the LSAs in a particular area.

asbrsummary—(Optional) Display summary AS boundary router LSA entries.

external—(Optional) Display external LSAs.

instance instance-name—(Optional) Display all OSPF database information under the named routing instance.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id lsa-id—(Optional) Display the LSA with the specified LSA identifier.

netsummary—(Optional) Display summary network LSAs.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

opaque-area—(Optional) Display opaque area-scope LSAs.

router—(Optional) Display information about router LSAs.

<table>
<thead>
<tr>
<th>Required Privilege</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>view</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear (ospf</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ospf database on page 2183</td>
</tr>
<tr>
<td>show ospf database on page 2184</td>
</tr>
<tr>
<td>show ospf database brief on page 2184</td>
</tr>
<tr>
<td>show ospf database detail on page 2184</td>
</tr>
<tr>
<td>show ospf database extensive on page 2185</td>
</tr>
<tr>
<td>show ospf database summary on page 2188</td>
</tr>
<tr>
<td>show ospf database opaque-area detail on page 2188</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Output Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 156 on page 2181 describes the output fields for the show ospf database command. Output fields are listed in the approximate order in which they appear.</td>
</tr>
</tbody>
</table>

**Table 156: show ospf database Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 156: `show ospf database` 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>Type</strong></td>
<td>Type of link advertisement: <code>ASBRSum</code>, <code>Extrem</code>, <code>Network</code>, <code>NSSA</code>, <code>OpaqArea</code>, <code>Router</code>, or <code>Summary</code>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Adv Rtr</strong></td>
<td>Address of the routing device that sent the advertisement.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Seq</strong></td>
<td>Link sequence number of the advertisement.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>Time elapsed since the LSA was originated, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Opt</strong></td>
<td>Optional OSPF capabilities associated with the LSA.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Cksum</strong></td>
<td>Checksum value of the LSA.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Len</strong></td>
<td>Length of the advertisement, in bytes.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Router</strong></td>
<td>Router link-state advertisement information:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• bits—Flags describing the routing device that generated the LSP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• link count—Number of links in the advertisement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• id—ID of a routing device or subnet on the link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• data—For stub networks, the subnet mask. Otherwise, the IP address of the routing device that generated the LSP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• type—Type of link. It can be <code>PointToPoint</code>, <code>Transit</code>, <code>Stub</code>, or <code>Virtual</code>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TOS count—Number of type-of-service (ToS) entries in the advertisement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TOS 0 metric—Metric for ToS 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TOS—Type-of-service (ToS) value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• metric—Metric for the ToS.</td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Network link-state advertisement information:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• mask—Network mask.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• attached router—ID of the attached neighbor.</td>
<td></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>Summary link-state advertisement information:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• mask—Network mask.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TOS—Type-of-service (ToS) value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• metric—Metric for the ToS.</td>
<td></td>
</tr>
<tr>
<td><strong>Gen timer</strong></td>
<td>How long until the LSA is regenerated.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Aging timer</strong></td>
<td>How long until the LSA expires.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Installed <code>hh:mm:ss</code> ago</strong></td>
<td>How long ago the route was installed.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 156: show ospf database 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>expires in hh:mm:ss</strong></td>
<td>How long until the route expires.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>sent hh:mm:ss ago</strong></td>
<td>How long ago the LSA was sent.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Last changed hh:mm:ss ago</strong></td>
<td>How long ago the route was changed.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Change count</strong></td>
<td>Number of times the route has changed.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Ours</strong></td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Router LSAs</strong></td>
<td>Number of router link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td><strong>Network LSAs</strong></td>
<td>Number of network link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td><strong>Summary LSAs</strong></td>
<td>Number of summary link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td><strong>NSSA LSAs</strong></td>
<td>Number of not-so-stubby area link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
</tbody>
</table>

### Sample Output

**show ospf database**

```
user@host>  show ospf database

OSPF link state database, Area 0.0.0.1
Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.70.103    10.255.70.103    0x80000002   215  0x20 0x4112  48
Router  *10.255.71.242    10.255.71.242    0x80000002   214  0x20 0x11b1  48
Summary *23.1.1.0        10.255.71.242    0x80000002   172  0x20 0x6d72  28
Summary *24.1.1.0        10.255.71.242    0x80000002   177  0x20 0x607e  28
NSSA    *33.1.1.1        10.255.71.242    0x80000002   217  0x20 0x73bd  36

OSPF link state database, Area 0.0.0.2
Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.71.52     10.255.71.52     0x80000004   174  0x20 0xd021  36
Router  *10.255.71.242    10.255.71.242    0x80000003   173  0x20 0xe191  36
Network *23.1.1.1        10.255.71.242    0x80000002   173  0x20 0x9c76  32
Summary *24.1.1.0        10.255.71.242    0x80000002   177  0x20 0xf37d  36
NSSA    *33.1.1.1        10.255.71.242    0x80000001   217  0x20 0xe047  36

OSPF link state database, Area 0.0.0.3
Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.71.238    10.255.71.238    0x80000003   179  0x20 0x3942  36
Router  *10.255.71.242    10.255.71.242    0x80000003   177  0x20 0xf37d  36
Network *24.1.1.1        10.255.71.242    0x80000002   177  0x20 0xc591  32
Summary *12.1.1.1        10.255.71.242    0x80000001   217  0x20 0xf3ee  36
Summary *23.1.1.0        10.255.71.242    0x80000002   172  0x20 0x6d72  28
NSSA    *33.1.1.1        10.255.71.242    0x80000001   222  0x20 0xeb3b  36
```
show ospf database

The output for `show ospf database nssa` with `nssa-only` configuration statement enabled at `[edit policy-options policy-statement policy-name term term-name then external]`, which clears P-bit on type 7 LSA.

```
user@host> show ospf database
OSPF link state database, Area 0.0.0.1

Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.70.103  10.255.70.103  0x80000002  215  0x20 0x4112  48
Router  *10.255.71.242  10.255.71.242  0x80000002  214  0x20 0x11b1  48
Summary *23.1.1.0     10.255.71.242  0x80000002  172  0x20 0x6d72  28
Summary *24.1.1.0     10.255.71.242  0x80000002  177  0x20 0x607e  28
NSSA    *33.1.1.1     10.255.71.242  0x80000002  217  0x20 0x73bd  36

OSPF link state database, Area 0.0.0.2

Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.71.52  10.255.71.52  0x80000004  174  0x20 0xd021  36
Router  *10.255.71.242  10.255.71.242  0x80000003  173  0x20 0xe191  36
Network *23.1.1.1     10.255.71.242  0x80000002  173  0x20 0x9c76  32
Summary *12.1.1.0     10.255.71.242  0x80000001  217  0x20 0xfeec  28
Summary *24.1.1.0     10.255.71.242  0x80000002  177  0x20 0x607e  28
NSSA    *33.1.1.1     10.255.71.242  0x80000001  222  0x20 0xe047  36

OSPF link state database, Area 0.0.0.3

Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router   10.255.71.238  10.255.71.238  0x80000003  179  0x20 0x3942  36
Router  *10.255.71.242  10.255.71.242  0x80000003  177  0x20 0xf37d  36
Network *24.1.1.1     10.255.71.242  0x80000002  177  0x20 0xc591  32
Summary *12.1.1.0     10.255.71.242  0x80000001  217  0x20 0xe047  36
Summary *23.1.1.0     10.255.71.242  0x80000002  172  0x20 0x6d72  28
NSSA    *33.1.1.1     10.255.71.242  0x80000001  222  0x20 0xeb3b  36
```

show ospf database brief

The output for the `show ospf database brief` command is identical to that for the `show ospf database` command. For sample output, see `show ospf database` on page 2183.

show ospf database detail

```
user@host> show ospf database detail
OSPF link state database, Area 0.0.0.1

Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
bits 0x0, link count 2
    id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Router  *10.255.71.242  10.255.71.242  0x80000002  260  0x20 0x11b1  48
bits 0x3, link count 2
    id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Summary *23.1.1.0     10.255.71.242  0x80000002  218  0x20 0x6d72  28

OSPF link state database, Area 0.0.0.2

bits 0x0, link count 2
    id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Router  *10.255.71.242  10.255.71.242  0x80000002  260  0x20 0x11b1  48
bits 0x3, link count 2
    id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Summary *23.1.1.0     10.255.71.242  0x80000002  218  0x20 0x6d72  28

OSPF link state database, Area 0.0.0.3

bits 0x0, link count 2
    id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Router  *10.255.71.242  10.255.71.242  0x80000002  260  0x20 0x11b1  48
bits 0x3, link count 2
    id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
    TOS count 0, TOS 0 metric 1
    id 12.1.1.0, data 255.255.255.0, Type Stub (3)
    TOS count 0, TOS 0 metric 1
Summary *23.1.1.0     10.255.71.242  0x80000002  218  0x20 0x6d72  28
```
show ospf database extensive

user@host> show ospf database extensive
### OSPF link state database, Area 0.0.0.1

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.70.103</td>
<td>10.255.70.103</td>
<td>0x80000002</td>
<td>286</td>
<td>0x20</td>
<td>0x4112</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>bits 0x0, link count 2</td>
<td>id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>id 12.1.1.0, data 255.255.255.0, Type Stub (3)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>Aging timer 00:55:14</td>
<td>Installed 00:04:43 ago, expires in 00:55:14</td>
</tr>
</tbody>
</table>

### Router *10.255.71.242*

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.242</td>
<td>10.255.71.242</td>
<td>0x80000002</td>
<td>285</td>
<td>0x20</td>
<td>0x11b1</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>bits 0x3, link count 2</td>
<td>id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>id 12.1.1.0, data 255.255.255.0, Type Stub (3)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>Gen timer 00:45:15</td>
<td>Aging timer 00:55:15</td>
</tr>
</tbody>
</table>

### Summary *23.1.1.0*

- mask 255.255.255.0
- TOs 0x0, metric 1
- Gen timer 00:45:57
- Aging timer 00:55:57
- Installed 00:04:03 ago, expires in 00:55:57, sent 00:04:01 ago
- Last changed 00:04:04 ago, Change count: 1, Ours

### Summary *24.1.1.0*

- mask 255.255.255.0
- TOs 0x0, metric 1
- Gen timer 00:45:52
- Aging timer 00:55:52
- Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
- Last changed 00:04:04 ago, Change count: 1, Ours

### NSSA *33.1.1.1*

- mask 255.255.255.255
- Type 2, TOs 0x0, metric 0, fwd addr 12.1.1.2, tag 0.0.0.0
- Gen timer 00:45:12
- Aging timer 00:55:12
- Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:48 ago
- Last changed 00:04:48 ago, Change count: 2, Ours

### OSPF link state database, Area 0.0.0.2

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.52</td>
<td>10.255.71.52</td>
<td>0x80000004</td>
<td>245</td>
<td>0x20</td>
<td>0xad021</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>bits 0x0, link count 1</td>
<td>id 23.1.1.1, data 23.1.1.2, Type Transit (2)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>Aging timer 00:55:55</td>
<td>Installed 00:04:02 ago, expires in 00:55:55</td>
<td>Last changed 00:04:02 ago, Change count: 2</td>
<td></td>
</tr>
</tbody>
</table>

### Router *10.255.71.242*

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.242</td>
<td>10.255.71.242</td>
<td>0x80000003</td>
<td>244</td>
<td>0x20</td>
<td>0xe191</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>bits 0x3, link count 1</td>
<td>id 23.1.1.1, data 23.1.1.1, Type Transit (2)</td>
<td>TOs count 0, TOS 0 metric 1</td>
<td>Gen timer 00:45:56</td>
<td>Aging timer 00:55:56</td>
<td>Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago</td>
<td>Last changed 00:04:04 ago, Change count: 2, Ours</td>
</tr>
</tbody>
</table>
Network *23.1.1.1         10.255.71.242    0x80000002   244  0x20 0x9c76  32
mask 255.255.255.0
attached router 10.255.71.242
attached router 10.255.71.52
Gen timer 00:45:56
Aging timer 00:55:56
Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago
Last changed 00:04:04 ago, Change count: 1, Ours
Summary *12.1.1.0         10.255.71.242    0x80000001   288  0x20 0xfeec  28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:12
Aging timer 00:55:12
Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:04 ago
Last changed 00:04:48 ago, Change count: 1, Ours
Summary *24.1.1.0         10.255.71.242    0x80000002   248  0x20 0x607e  28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:52
Aging timer 00:55:52
Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:04 ago
Last changed 00:04:08 ago, Change count: 1, Ours
NSSA    *33.1.1.1         10.255.71.242    0x80000001   293  0x28 0xe047  36
mask 255.255.255.255
Type 2, TOS 0x0, metric 0, fwd addr 23.1.1.1, tag 0.0.0.0
Gen timer 00:45:07
Aging timer 00:55:07
Installed 00:04:53 ago, expires in 00:55:07, sent 00:04:04 ago
Last changed 00:04:53 ago, Change count: 1, Ours

OSPF link state database, Area 0.0.0.3

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.238</td>
<td>10.255.71.238</td>
<td>0x80000003</td>
<td>250</td>
<td>0x20</td>
<td>0x3942</td>
<td>36</td>
</tr>
<tr>
<td>bits 0x0, link count 1</td>
<td>id 24.1.1.1, data 24.1.1.2, Type Transit (2)</td>
<td>TOS count 0, TOS 0 metric 1</td>
<td>Aging timer 00:55:50</td>
<td>Installed 00:04:07 ago, expires in 00:55:50</td>
<td>Last changed 00:04:07 ago, Change count: 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>*10.255.71.242</td>
<td>10.255.71.242</td>
<td>0x80000003</td>
<td>248</td>
<td>0x20</td>
<td>0xf37d</td>
<td>36</td>
</tr>
<tr>
<td>bits 0x3, link count 1</td>
<td>id 24.1.1.1, data 24.1.1.1, Type Transit (2)</td>
<td>TOS count 0, TOS 0 metric 1</td>
<td>Gen timer 00:45:52</td>
<td>Aging timer 00:55:52</td>
<td>Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago</td>
<td>Last changed 00:04:08 ago, Change count: 2, Ours</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>*24.1.1.1</td>
<td>10.255.71.242</td>
<td>0x80000002</td>
<td>248</td>
<td>0x20</td>
<td>0xc591</td>
<td>32</td>
</tr>
<tr>
<td>mask 255.255.255.0</td>
<td>attached router 10.255.71.242</td>
<td>attached router 10.255.71.238</td>
<td>Gen timer 00:45:52</td>
<td>Aging timer 00:55:52</td>
<td>Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago</td>
<td>Last changed 00:04:08 ago, Change count: 1, Ours</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>*12.1.1.0</td>
<td>10.255.71.242</td>
<td>0x80000001</td>
<td>288</td>
<td>0x20</td>
<td>0xfeec</td>
<td>28</td>
</tr>
<tr>
<td>mask 255.255.255.0</td>
<td>TOS 0x0, metric 1</td>
<td>Gen timer 00:45:12</td>
<td>Aging timer 00:55:12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show ospf database summary

user@host> show ospf database summary

Area 0.0.0.1:
  2 Router LSAs
  2 Summary LSAs
  1 NSSA LSAs
Area 0.0.0.2:
  2 Router LSAs
  1 Network LSAs
  2 Summary LSAs
  1 NSSA LSAs
Area 0.0.0.3:
  2 Router LSAs
  1 Network LSAs
  2 Summary LSAs
  1 NSSA LSAs
Externals:
  Interface fe-2/2/1.0:
  Interface ge-0/3/2.0:
  Interface so-0/1/2.0:
  Interface so-0/1/2.0:

show ospf database opaque-area detail

user@host> show ospf database opaque-area detail

OSPF database, Area 0.0.0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpaqArea*4.0.0.0</td>
<td>1.1.1.10</td>
<td>0x800000ef</td>
<td>1510</td>
<td>0x22</td>
<td>0x2810</td>
<td>156</td>
<td></td>
</tr>
</tbody>
</table>

Area-opaque LSA
SR-Algorithm (8), length 1:
  Algo (1), length 1:
    0
SID/Label Range (9), length 12:
  Range Size (1), length 3:
    256
  SID/Label (1), length 3:
    Label (1), length 3:
      802048
  SID/Label Range (9), length 12:
Range Size (1), length 3:
SID/Label (1), length 3:
  Label (1), length 3:
  802304
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  802560
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  802816
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  803072
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  803328
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  803584
SID/Label Range (9), length 12:
  Range Size (1), length 3:
  256
  SID/Label (1), length 3:
  Label (1), length 3:
  803840

The Extended Prefix LSA (eg):

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpaqArea*7.0.0.1</td>
<td>10.10.10.10</td>
<td>0x80000002</td>
<td>561</td>
<td>0x22</td>
<td>0x60eb</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>

Area-opaque LSA

Extended Prefix (1), length 20:
  Route Type (1), length 1:
    1
  Prefix Length (2), length 1:
    32
  AF (3), length 1:
    0
  Flags (4), length 1:
    0x40
  Prefix (5), length 32:
    10.10.10.10
  Prefix Sid (2), length 8:
    Flags (1), length 1:
OSPF database, Area 0.0.0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpaqArea*7.0.0.1</td>
<td>80.0.0.4</td>
<td>0x800000054</td>
<td>1095</td>
<td>0x22</td>
<td>0x29c</td>
<td></td>
<td>44</td>
</tr>
<tr>
<td>Area-opaque LSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Prefix (1), length 20:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Route Type (1), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix Length (2), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AF (3), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags (4), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix (5), length 32:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix Sid (2), length 8:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags (1), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT ID (2), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Algorithm (3), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SID (4), length 4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpaqArea 8.0.0.1</td>
<td>1.1.1.1</td>
<td>0x800000001</td>
<td>688</td>
<td>0x22</td>
<td>0xcd8a</td>
<td></td>
<td>48</td>
</tr>
<tr>
<td>Area-opaque LSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Link (1), length 24:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Type (1), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Id (2), length 4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Data (3), length 4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjacency Sid (2), length 7:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags (1), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT ID (2), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Algorithm (3), length 1:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SID (4), length 4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Label (4), length 3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**show ospf3 database**

**List of Syntax**  
Syntax on page 2191  
Syntax (EX Series Switches and QFX Series) on page 2191

**Syntax**
```
show ospf3 database
  <brief | detail | extensive | summary>
  <advertising-router (address | self)>
  <area area-id>
  <external>
  <instance instance-name>
  <inter-area-prefix>
  <inter-area-router>
  <intra-area-prefix>
  <link>
  <link-local>
  <logical-system (all | logical-system-name)>
  <lsa-id lsa-id>
  <network>
  <nssa>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
  <router>
```

**Syntax (EX Series Switches and QFX Series)**
```
show ospf3 database
  <brief | detail | extensive | summary>
  <advertising-router (address | self)>
  <area area-id>
  <external>
  <instance instance-name>
  <inter-area-prefix>
  <inter-area-router>
  <intra-area-prefix>
  <link>
  <link-local>
  <logical-system (all | logical-system-name)>
  <lsa-id lsa-id>
  <network>
  <nssa>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
  <router>
```

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
**realm** option introduced in Junos OS Release 9.2.  
**advertising-router (address | self)** option introduced in Junos Release 9.5.  
**advertising-router (address | self)** option introduced in Junos OS Release 9.5 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**  
Display the entries in the OSPF version 3 (OSPFv3) link-state database, which contains data about link-state advertisement (LSA) packets.
Options

none—Display standard information about all entries in the OSPFv3 link-state database.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

advertising-router (address | self)—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.

area area-id—(Optional) Display the LSAs in a particular area.

external—(Optional) Display external LSAs.

instance instance-name—(Optional) Display all OSPF database information under the named routing instance.

inter-area-prefix—(Optional) Display information about inter-area-prefix LSAs.

inter-area-router—(Optional) Display information about inter-area-router LSAs.

intra-area-prefix—(Optional) Display information about intra-area-prefix LSAs.

link—(Optional) Display information about link LSAs.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id lsa-id—(Optional) Display the LSA with the specified LSA identifier.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) Display information about the specified OSPFv3 realm, or address family. Use the realm option to specify an address family other than IPv6 unicast, which is the default.

router—(Optional) Display information about router LSAs.

Required Privilege
Level
view

Related
Documentation
• clear (ospf | ospf3) database on page 2154

List of Sample Output
show ospf3 database brief on page 2197
show ospf3 database extensive on page 2198
show ospf3 database summary on page 2200

Output Fields
Table 157 on page 2193 lists the output fields for the show ospf3 database command. Output fields are listed in the approximate order in which they appear.
Table 157: show ospf3 database Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OSPF link state database, area area-number</strong></td>
<td>Entries in the link-state database for this area.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>OSPF AS SCOPE link state database</strong></td>
<td>Entries in the AS scope link-state database.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>OSPF Link-Local link state database, interface interface-name</strong></td>
<td>Entries in the link-local link-state database for this interface.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>area</strong></td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of link advertisement: Extern, InterArPfx, InterArRtr, IntraArPrx, Link, Network, NSSA, or Router.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Link identifier included in the advertisement. An asterisk (*) preceding the identifier marks database entries that originated from the local routing device.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Adv Rtr</strong></td>
<td>Address of the routing device that sent the advertisement.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Seq</strong></td>
<td>Link sequence number of the advertisement.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>Time elapsed since the LSA was originated, in seconds.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Cksum</strong></td>
<td>Checksum value of the LSA.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Len</strong></td>
<td>Length of the advertisement, in bytes.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Router (Router Link-State Advertisements)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>bits</strong></td>
<td>Flags describing the routing device that generated the LSP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>Option bits carried in the router LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>For Each Router Link</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of interface. The value of all other output fields describing a routing device interface depends on the interface’s type:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• PointToPoint (1)—Point-to-point connection to another routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transit (2)—Connection to a transit network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual (4)—Virtual link.</td>
<td></td>
</tr>
<tr>
<td><strong>Loc-if-id</strong></td>
<td>Local interface ID assigned to the interface that uniquely identifies the interface with the routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Nbr-if-id</strong></td>
<td>Interface ID of the neighbor’s interface for this routing device link.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 157: `show ospf3 database` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nbr-rtr-id</td>
<td>Router ID of the neighbor routing device (for type 2 interfaces, the attached link’s designated router).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of the router link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed <code>nn:nn:nn</code> ago</td>
<td>How long ago the route was installed, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in <code>nn:nn:nn</code></td>
<td>How long until the route expires, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent <code>nn:nn:nn</code> ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

**Network (Network Link-State Advertisements)**

<table>
<thead>
<tr>
<th>Options</th>
<th>Option bits carried in the network LSA.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attached Router</td>
<td>Router IDs of each of the routing devices attached to the link. Only routing devices that are fully adjacent to the designated router are listed. The designated router includes itself in this list.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**InterArPfx (Interarea-Prefix Link-State Advertisements)**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>IPv6 address prefix.</th>
<th>detail extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed <code>nn:nn:nn</code> ago</td>
<td>How long ago the route was installed, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in <code>nn:nn:nn</code></td>
<td>How long until the route expires, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent <code>nn:nn:nn</code> ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format <code>hours:minutes:seconds</code>.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 157: show ospf3 database 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>Ours</strong></td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>InterArRtr (Interarea-Router Link-State Advertisements)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dest-router-id</td>
<td>Router ID of the routing device described by the LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>options</td>
<td>Optional capabilities supported by the routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Extern (External Link-State Advertisements)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of the route, which depends on the value of Type.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type n</td>
<td>Type of external metric: Type 1 or Type 2.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed nn:nn:nn ago</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in nn:nn:nn</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent nn:nn:nn ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Link (Link-State Advertisements)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6-Address</td>
<td>IPv6 link-local address on the link for which this link LSA originated.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Options</td>
<td>Option bits carried in the link LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>priority</td>
<td>Router priority of the interface attaching the originating routing device to the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 157: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed nn:nn:nn ago</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in nn:nn</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent nn:nn:nn ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

IntraArPfx (Intra-Area-Prefix Link-State Advertisements)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref-lsa-type</td>
<td>LSA type of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>• Router</td>
<td>Address prefixes are associated with a router LSA.</td>
<td></td>
</tr>
<tr>
<td>• Network</td>
<td>Address prefixes are associated with a network LSA.</td>
<td></td>
</tr>
<tr>
<td>Ref-lsa-id</td>
<td>Link-state ID of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Ref-router-id</td>
<td>Advertising router ID of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of this prefix. Expressed in the same units as the interface costs in the router LSAs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed hh:mm:ss ago</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in hh:mm:ss</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent hh:mm:ss ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 157: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>*n Router LSAs</td>
<td>Number of router LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>*n Network LSAs</td>
<td>Number of network LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>*n InterArPfx LSAs</td>
<td>Number of interarea-prefix LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>*n InterArRtr LSAs</td>
<td>Number of interarea-router LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>*n IntraArPfx LSAs</td>
<td>Number of intra-area-prefix LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Externals</td>
<td>Display of the external LSA database.</td>
<td>summary</td>
</tr>
<tr>
<td>*n Extern LSAs</td>
<td>Number of external LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Interface interface-name</td>
<td>Name of the interface for which link-local LSA information is displayed.</td>
<td>summary</td>
</tr>
<tr>
<td>*n Link LSAs</td>
<td>Number of link LSAs in the link-state database.</td>
<td>summary</td>
</tr>
</tbody>
</table>

Sample Output

show ospf3 database brief

```
user@host> show ospf3 database brief

OSPF3 link state database, area 0.0.0.0
Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Router      0.0.0.1          10.255.4.85      0x80000003   885  0xa697  40
Router     *0.0.0.1          10.255.4.93      0x80000002   953  0xc677  40
InterArPfx *0.0.0.1          10.255.4.93      0x80000001   910  0xb96f  44
InterArRtr *0.0.0.1          10.255.4.93      0x80000001   910  0xe159  32
IntraArPfx *0.0.0.1          10.255.4.93      0x80000002   432  0x788f  72

OSPF3 link state database, area 0.0.0.1
Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Router     *0.0.0.1          10.255.4.93      0x80000003   916  0xea40  40
Router      0.0.0.1          10.255.4.97      0x80000006   851  0xc95b  40
Network    0.0.0.1          10.255.4.97      0x80000002   916  0x4598  32
InterArPfx *0.0.0.1          10.255.4.93      0x80000002   117  0xa980  44
InterArPfx *0.0.0.2          10.255.4.93      0x80000002   62   0xd47e  44
NSSA       0.0.0.1          10.255.4.97      0x80000002   362  0x45ee  44
IntraArPfx 0.0.0.1          10.255.4.97      0x80000006   851  0x2f77  52

OSPF3 AS SCOPE link state database
Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Extern     *0.0.0.1          10.255.4.85      0x80000002   63   0x9b86  44
Extern     *0.0.0.1          10.255.4.93      0x80000001   910  0x59c9  44

OSPF3 Link-Local link state database, interface ge-1/3/0.0
Type       ID               Adv Rtr           Seq         Age  Cksum  Len
Link        *0.0.0.2          10.255.4.93      0x80000003   916  0x4dab  64
```
```bash
user@host> show ospf3 database extensive

OSPF3 link state database, area 0.0.0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>0.0.0.1</td>
<td>10.255.4.85</td>
<td>0x80000003</td>
<td>1028</td>
<td>0xa697</td>
<td>40</td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td>Router  *0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>1096</td>
<td>0xc677</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx *0.0.0.2</td>
<td>10.255.4.93</td>
<td>0x80000001</td>
<td>1053</td>
<td>0xdb96f</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx *0.0.0.3</td>
<td>10.255.4.93</td>
<td>0x80000001</td>
<td>1053</td>
<td>0x71d3</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArRtr *0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000001</td>
<td>1053</td>
<td>0xe159</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx 0.0.0.1</td>
<td>10.255.4.85</td>
<td>0x80000002</td>
<td>1028</td>
<td>0x2403</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx *0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>575</td>
<td>0x788f</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OSPF3 link state database, area 0.0.0.1
```
<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>*0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000003</td>
<td>1059</td>
<td>0xea40</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>bits 0x3, Options 0x19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type Transit (2), Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loc-If-Id 2, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gen timer 00:08:51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:42:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:17:39 ago, expires in 00:42:21, sent 00:17:37 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>0.0.0.1</td>
<td>10.255.4.97</td>
<td>0x80000006</td>
<td>994</td>
<td>0xc95b</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>bits 0x2, Options 0x19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type Transit (2), Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loc-If-Id 2, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:43:25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>0.0.0.2</td>
<td>10.255.4.97</td>
<td>0x80000002</td>
<td>1059</td>
<td>0x4598</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>Options 0x11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attached router 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attached router 10.255.4.93</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:42:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>*0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>260</td>
<td>0xa980</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Prefix feee::10:10:1/126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x0, Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gen timer 00:45:39</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:55:39</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:04:20 ago, expires in 00:55:40, sent 00:04:18 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>*0.0.0.2</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>205</td>
<td>0xd47e</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Prefix feee::10:255:4:93/128</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x0, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gen timer 00:46:35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:56:35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:03:25 ago, expires in 00:56:35, sent 00:03:23 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>*0.0.0.3</td>
<td>10.255.4.93</td>
<td>0x80000001</td>
<td>1089</td>
<td>0x9bbb</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Prefix feee::10:255:4:85/128</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x0, Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gen timer 00:04:46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:41:51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:18:09 ago, expires in 00:41:51, sent 00:17:43 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ours</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSSA</td>
<td>0.0.0.1</td>
<td>10.255.4.97</td>
<td>0x80000002</td>
<td>505</td>
<td>0x45ee</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Prefix feee::200:200:1:0/124</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x8, Metric 10, Type 2,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:51:35</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:08:22 ago, expires in 00:51:35, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx</td>
<td>0.0.0.1</td>
<td>10.255.4.97</td>
<td>0x80000006</td>
<td>994</td>
<td>0x2f77</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-count 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix feee::10:255:4:97/128</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x2, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:43:25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx</td>
<td>0.0.0.3</td>
<td>10.255.4.97</td>
<td>0x80000002</td>
<td>1059</td>
<td>0x4446</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Ref-lsa-type Network, Ref-lsa-id 0.0.0.2, Ref-router-id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-count 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix feee::10:10:2:0/126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prefix-options 0x0, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:42:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OSPF3 AS SCOPE link state database

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extern</td>
<td>0.0.0.1</td>
<td>10.255.4.85</td>
<td>0x80000002</td>
<td>206</td>
<td>0x9b86</td>
<td>44</td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::100:100:1:0/124</td>
<td>Metric 20, Type 2, Aging timer 00:56:34</td>
<td>Installed 00:03:23 ago, expires in 00:56:34, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>*0.0.0.1</td>
<td>10.255.4.93</td>
<td>0x80000001</td>
<td>1053</td>
<td>0x59c9</td>
<td>44</td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::200:200:1:0/124</td>
<td>Metric 20, Type 2, Aging timer 00:42:26</td>
<td>Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OSPF3 Link-Local link state database, interface ge-1/3/0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.2</td>
<td>10.255.4.93</td>
<td>0x80000003</td>
<td>205</td>
<td>0xa87d</td>
<td>64</td>
</tr>
<tr>
<td>fe80::290:69ff:fe39:1cdb</td>
<td>Options 0x11, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:2/126</td>
<td>Prefix-options 0x0</td>
<td>Gen timer 00:12:56</td>
<td>Aging timer 00:42:20</td>
</tr>
<tr>
<td>Link</td>
<td>0.0.0.2</td>
<td>10.255.4.97</td>
<td>0x80000003</td>
<td>205</td>
<td>0xa87d</td>
<td>64</td>
</tr>
<tr>
<td>fe80::290:69ff:fe38:883e</td>
<td>Options 0x11, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:2/126</td>
<td>Prefix-options 0x0</td>
<td>Gen timer 00:56:35</td>
<td>Aging timer 00:03:22 ago, expires in 00:56:35, sent 02:37:54 ago</td>
</tr>
</tbody>
</table>

OSPF3 Link-Local link state database, interface so-2/2/0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.3</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>505</td>
<td>0x6b7a</td>
<td>64</td>
</tr>
<tr>
<td>fe80::280:42ff:fe10:f169</td>
<td>Options 0x13, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:1/126</td>
<td>Prefix-options 0x0</td>
<td>Gen timer 00:51:34</td>
<td>Aging timer 00:08:23 ago, expires in 00:51:34, sent 02:37:54 ago</td>
</tr>
<tr>
<td>Link</td>
<td>0.0.0.3</td>
<td>10.255.4.93</td>
<td>0x80000002</td>
<td>505</td>
<td>0x6b7a</td>
<td>64</td>
</tr>
<tr>
<td>fe80::280:42ff:fe10:f177</td>
<td>Options 0x13, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:1/126</td>
<td>Prefix-options 0x0</td>
<td>Gen timer 00:37:28</td>
<td>Aging timer 00:51:35</td>
</tr>
</tbody>
</table>

show ospf3 database summary

user@host> show ospf3 database summary

Area 0.0.0.0:
- 2 Router LSAs
- 1 InterArPfx LSAs
- 1 InterArRtr LSAs
- 1 IntraArPfx LSAs
Area 0.0.0.1:
  2 Router LSAs
  1 Network LSAs
  2 InterArPfx LSAs
  1 NSSA LSAs
  1 IntraArPfx LSAs
Externals:
  2 Extern LSAs
Interface ge-1/3/0.0:
  1 Link LSAs
Interface lo0.0:
Interface so-2/2/0.0:
  1 Link LSAs
show (ospf | ospf3) interface

**List of Syntax**

Syntax on page 2202
Syntax (EX Series Switches and QFX Series) on page 2202

**Syntax**

```
show (ospf | ospf3) interface
  <brief | detail | extensive>
  <area area-id>
  <interface-name>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

**Syntax (EX Series Switches and QFX Series)**

```
show (ospf | ospf3) interface
  <brief | detail | extensive>
  <area area-id>
  <interface-name>
  <instance instance-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
area option introduced in Junos OS Release 9.2.
area option introduced in Junos OS Release 9.2 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display the status of OSPF interfaces.

**Options**

- **none**—Display standard information about the status of all OSPF interfaces for all routing instances
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **area area-id**—(Optional) Display information about the interfaces that belong to the specified area.
- **interface-name**—(Optional) Display information for the specified interface.
- **instance instance-name**—(Optional) Display all OSPF interfaces under the named routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(OSPFv3 only) (Optional) Display information about the interfaces for the specified OSPFv3 realm, or address
family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege Level**
- **view**

**List of Sample Output**
- `show ospf interface brief` on page 2205
- `show ospf interface detail` on page 2205
- `show ospf3 interface detail` on page 2205
- `show ospf interface detail (When Multiarea Adjacency Is Configured)` on page 2206
- `show ospf interface extensive (When Flooding Reduction Is Enabled)` on page 2207
- `show ospf interface extensive (When LDP Synchronization Is Configured)` on page 2207

**Output Fields**
Table 158 on page 2203 lists the output fields for the `show (ospf | ospf3) interface` command. Output fields are listed in the approximate order in which they appear.

**Table 158: show (ospf | ospf3) 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>Name of the interface running OSPF version 2 or OSPF version 3.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: BDR, Down, DR, DROther, Loop, PtToPt, or Waiting.</td>
<td>All levels</td>
</tr>
<tr>
<td>Area</td>
<td>Number of the area that the interface is in.</td>
<td>All levels</td>
</tr>
<tr>
<td>DR ID</td>
<td>Address of the area's designated router.</td>
<td>All levels</td>
</tr>
<tr>
<td>BDR ID</td>
<td>Backup designated router for a particular subnet.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nbrs</td>
<td>Number of neighbors on this interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface: LAN, NBMA, P2MP, P2P, or Virtual.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mask</td>
<td>Netmask of the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-length</td>
<td>(OSPFv3) IPv6 prefix length, in bits.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>OSPF3-Intf-index</td>
<td>(OSPFv3) OSPF version 3 interface index.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>Interface maximum transmission unit (MTU).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Cost</td>
<td>Interface cost (metric).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DR addr</td>
<td>Address of the designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>BDR addr</td>
<td>Address of the backup designated router.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 158: show (ospf | ospf3) 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>Adj count</td>
<td>Number of adjacent neighbors.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Secondary</td>
<td>Indicates that this interface is configured as a secondary interface for this area. This interface can belong to more than one area, but can be designated as a primary interface for only one area.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flood Reduction</td>
<td>Indicates that this interface is configured with flooding reduction. All self-originated LSAs from this interface are initially sent with the DoNotAge bit set. As a result, LSAs are refreshed only when a change occurs.</td>
<td>extensive</td>
</tr>
<tr>
<td>Priority</td>
<td>Router priority used in designated router (DR) election on this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flood list</td>
<td>List of link-state advertisements (LSAs) that might be about to flood this interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ack list</td>
<td>Acknowledgment list. List of pending acknowledgments on this interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Descriptor list</td>
<td>List of packet descriptors.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hello</td>
<td>Configured value for the hello timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Dead</td>
<td>Configured value for the dead timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Auth type</td>
<td>(OSPFv2) Authentication mechanism for sending and receiving OSPF protocol packets:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• MD5—The MD5 mechanism is configured in accordance with RFC 2328.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None—No authentication method is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password—A simple password (RFC 2328) is configured.</td>
<td></td>
</tr>
<tr>
<td>Topology</td>
<td>(Multiarea adjacency) Name of topology: default or name.</td>
<td></td>
</tr>
<tr>
<td>LDP sync state</td>
<td>(OSPFv2 and LDP synchronization) Current state of LDP synchronization: in sync. in holddown, and not supported.</td>
<td>extensive</td>
</tr>
<tr>
<td>reason</td>
<td>(OSPFv2 and LDP synchronization) Reason for the current state of LDP synchronization. The LDP session might be up or down, or adjacency might be up or down.</td>
<td>extensive</td>
</tr>
<tr>
<td>config holdtime</td>
<td>(OSPFv2 and LDP synchronization) Configured value of the hold timer.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>If the state is not synchronized, and the hold time is not infinity, the remaining field displays the number of seconds that remain until the configured hold timer expires.</td>
<td></td>
</tr>
<tr>
<td>IPSec SA name</td>
<td>(OSPFv2) Name of the IPSec security association name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Active key ID</td>
<td>(OSPFv2 and MD5) Number from 0 to 255 that uniquely identifies an MD5 key.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 158: show (ospf | ospf3) 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>Start time</strong></td>
<td>(OSPFv2 and MD5) Time at which the routing device starts using an MD5 key to authenticate OSPF packets transmitted on the interface on which this key is configured. To authenticate received OSPF protocol packets, the key becomes effective immediately after the configuration is committed. If the start time option is not configured, the key is effective immediately for send and receive and is displayed as Start time 1970 Jan 01 00:00:00 PST.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>ReXmit</strong></td>
<td>Configured value for the Retransmit timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Stub, Not Stub, or Stub NSSA</strong></td>
<td>Type of area.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

#### Sample Output

**show ospf interface brief**

```
   show ospf interface brief

user@host> show ospf interface brief

Interface            State  Area           DR ID            BDR ID Nbrs
at-5/1/0.0            PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 1
ge-2/3/0.0            DR     0.0.0.0         192.168.4.16    192.168.4.15 1
lo0.0                 Down  0.0.0.0         192.168.4.16    0.0.0.0 0
so-0/0/0.0             PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 0
so-6/0/1.0             PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 1
so-6/0/2.0             Down  0.0.0.0         0.0.0.0          0.0.0.0 0
so-6/0/3.0             PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 1
```

**show ospf interface detail**

```
   show ospf interface detail

user@host> show ospf interface detail

Interface            State  Area           DR-ID  BDR-ID Nbrs
fe-0/0/1.0             BDR    0.0.0.0         192.168.37.12 10.255.245.215 1
Type LAN, address 192.168.37.11, Mask 255.255.255.248, MTU 4460, Cost 40
DR addr 192.168.37.12, BDR addr 192.168.37.11, Adj count 1, Priority 128
Hello 10, Dead 40, ReXmit 5, Not Stub

   t1-0/2/1.0             PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 0
Type P2P, Address 0.0.0.0, Mask 0.0.0.0, MTU 1500, Cost 2604
    Adj count 0
   Hello 10, Dead 40, ReXmit 5, Not Stub
   Auth type: MD5, Active key ID 3, Start time 2002 Nov 19 10:00:00 PST
   IPSec SA Name: sa
```

**show ospf3 interface detail**

```
   user@host> show ospf3 interface so-0/0/3.0 detail

Interface            State  Area           DR-ID  BDR-ID Nbrs
so-0/0/3.0             PtToPt 0.0.0.0        0.0.0.0          0.0.0.0 1
Address fe80::2a0:a5ff:fe28:1dfc, Prefix-length 64
OSPF3-Intf-index 1, Type P2P, MTU 4470, Cost 12, Adj-count 1
   Hello 10, Dead 40, ReXmit 5, Not Stub
```
show ospf interface detail
(When Multiarea Adjacency Is Configured)

```
user@host> show ospf interface detail
user@host> show ospf interface detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>10.255.245.2</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Type: LAN, Address: 127.0.0.1, Mask: 255.255.255.255, MTU: 65535, Cost: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hello: 10, Dead: 40, ReXmit: 5, Not Stub</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auth type: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Topology default (ID 0) -&gt; Cost: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| lo0.0     | DR    | 0.0.0.0| 10.255.245.2 | 0.0.0.0 | 0    |
|           | Type: LAN, Address: 10.255.245.2, Mask: 255.255.255.255, MTU: 65535, Cost: 0 |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: None |
|           | Topology default (ID 0) -> Cost: 0 |

| so-0/0/0.0| PtToPt| 0.0.0.0| 0.0.0.0 | 0.0.0.0 | 1    |
|           | Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1 |
|           | Adj count: 1 |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: Passive |
|           | Topology default (ID 0) -> Cost: 1 |

| so-0/0/0.0| PtToPt| 0.0.0.0| 0.0.0.0 | 0.0.0.0 | 0    |
|           | Type: P2P, Address: 192.168.37.46, Mask: 255.255.255.254, MTU: 4470, Cost: 1 |
|           | Adj count: 0, Passive |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: None |
|           | Topology default (ID 0) -> Passive, Cost: 1 |

| so-1/0/0.0| PtToPt| 0.0.0.0| 0.0.0.0 | 0.0.0.0 | 1    |
|           | Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1 |
|           | Adj count: 1 |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: None |
|           | Topology default (ID 0) -> Cost: 1 |

| so-1/0/0.0| PtToPt| 0.0.0.0| 0.0.0.0 | 0.0.0.0 | 0    |
|           | Type: P2P, Address: 192.168.37.54, Mask: 255.255.255.254, MTU: 4470, Cost: 1 |
|           | Adj count: 0, Passive |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: None |
|           | Topology default (ID 0) -> Passive, Cost: 1 |

| so-0/0/0.0| PtToPt| 1.1.1.1| 0.0.0.0 | 0.0.0.0 | 1    |
|           | Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1 |
|           | Adj count: 1, Secondary |
|           | Hello: 10, Dead: 40, ReXmit: 5, Not Stub |
|           | Auth type: None |
|           | Topology default (ID 0) -> Cost: 1 |

| so-1/0/0.0| PtToPt| 1.1.1.1| 0.0.0.0 | 0.0.0.0 | 1    |
|           | Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1 |
|           | Adj count: 1, Secondary |
```
show ospf interface area area-id

```
user@host> show ospf interface area 1.1.1.1
Interface          State   Area            DR ID           BDR ID          Nbrs
so-0/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1
so-1/0/0.0          PtToPt  1.1.1.1         0.0.0.0         0.0.0.0            1
```

show ospf interface extensive
(When Flooding Reduction Is Enabled)

```
user@host> show ospf interface extensive
Interface              State     Area            DR ID           BDR ID
fe-0/0/0.0              PtToPt  0.0.0.0         0.0.0.0         0.0.0.0

Type: P2P, Address: 10.10.10.1, Mask: 255.255.255.0, MTU: 1500, Cost: 1
Adj count: 0
Secondary, Flood Reduction
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
```

show ospf interface extensive
(When LDP Synchronization Is Configured)

```
user@host> show ospf interface extensive
Interface              State     Area            DR ID           BDR ID
Nbrs
so-1/0/3.0              Down  0.0.0.0         0.0.0.0         0.0.0.0
0

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 65535
Adj count: 0
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
LDP sync state: in holddown, for: 00:00:08, reason: LDP down during config
  config holdtime: 10 seconds, remaining: 1
```
show (ospf | ospf3) io-statistics

**List of Syntax**
Syntax on page 2208
Syntax (EX Series Switch and QFX Series) on page 2208

**Syntax**
show (ospf | ospf3) io-statistics
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switch and QFX Series)**
show (ospf | ospf3) io-statistics

**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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display Open Shortest Path First (OSPF) input and output statistics.

**Options**
none—Display OSPF input and output statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**Related Documentation**
- clear (ospf | ospf3) statistics on page 2161

**List of Sample Output**
show ospf io-statistics on page 2209

**Output Fields**
Table 159 on page 2208 lists the output fields for the show ospf io-statistics command. Output fields are listed in the approximate order in which they appear.

**Table 159: show (ospf | ospf3) io-statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets read</td>
<td>Number of OSPF packets read since the last time the routing protocol was started.</td>
</tr>
<tr>
<td>average per run</td>
<td>Total number of packets divided by the total number of times the OSPF read operation is scheduled to run.</td>
</tr>
<tr>
<td>max run</td>
<td>Maximum number of packets for a given run among all scheduled runs.</td>
</tr>
</tbody>
</table>
### Table 159: show (ospf | ospf3) io-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive errors</td>
<td>Number of faulty packets received with errors.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ospf io-statistics**

```
user@host> show ospf io-statistics

Packets read: 7361, average per run: 1.00, max run: 1
Receive errors:
    None
```
show (ospf | ospf3) log

**List of Syntax**
Syntax on page 2210
Syntax (EX Series Switch and QFX Series) on page 2210

**Syntax**

```plaintext
show (ospf | ospf3) log
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
  <topology topology-name>
```

**Syntax (EX Series Switch and QFX Series)**

```plaintext
show (ospf | ospf3) log
  <instance instance-name>
  <topology topology-name>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
topology option introduced in Junos OS Release 9.0.
topology option introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display the entries in the Open Shortest Path First (OSPF) log of SPF calculations.

**Options**

- none—Display entries in the OSPF log of SPF calculations for all routing instances.
- instance instance-name—(Optional) Display entries for the specified routing instance.
- logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
- topology topology-name—(Optional) (OSPFv2 only) Display entries for the specified topology.
- realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display entries for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege**
view

**List of Sample Output**
show ospf log on page 2211
show ospf log topology voice on page 2211
Output Fields

Table 160 on page 221 lists the output fields for the `show (ospf | ospf3) log` command. Output fields are listed in the approximate order in which they appear.

Table 160: `show (ospf | ospf3) log` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When</strong></td>
<td>Time, in weeks (w) and days (d), since the SPF calculation was made.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of calculation: Cleanup, External, Interarea, NSSA, Redist, SPF, Stub, Total, or VirtualLink.</td>
</tr>
<tr>
<td><strong>Elapsed</strong></td>
<td>Amount of time, in seconds, that elapsed during the operation, or the time required to complete the SPF calculation. The start time is the time displayed in the <strong>When</strong> field.</td>
</tr>
</tbody>
</table>

Sample Output

**show ospf log**

```
user@host> show ospf log
When    Type     Elapsed
-------- ------     -------
1w4d 17:25:58 Stub  0.000017
1w4d 17:25:58 SPF    0.000070
1w4d 17:25:58 Stub   0.000019
1w4d 17:25:58 Interarea 0.000054
1w4d 17:25:58 External 0.000005
1w4d 17:25:58 Cleanup 0.000203
1w4d 17:25:58 Total   0.000537
1w4d 17:24:48 SPF    0.000125
1w4d 17:24:48 Stub   0.000017
1w4d 17:24:48 SPF    0.000100
1w4d 17:24:48 Stub   0.000016
1w4d 17:24:48 Interarea 0.000056
1w4d 17:24:48 External 0.000005
1w4d 17:24:48 Cleanup 0.000238
1w4d 17:24:48 Total   0.000600
...
```

**show ospf log topology voice**

```
user@host> show ospf log topology voice
Topology voice SPF log:

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:06:11</td>
<td>SPF</td>
<td>0.000116</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Stub</td>
<td>0.000114</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Interarea</td>
<td>0.000126</td>
</tr>
<tr>
<td>00:06:11</td>
<td>External</td>
<td>0.000067</td>
</tr>
<tr>
<td>00:06:11</td>
<td>NSSA</td>
<td>0.000037</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Cleanup</td>
<td>0.000186</td>
</tr>
</tbody>
</table>
```
### Maximum length of each event type

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:43</td>
<td>SPF</td>
<td>0.000140</td>
</tr>
<tr>
<td>00:13:33</td>
<td>Stub</td>
<td>0.000116</td>
</tr>
<tr>
<td>00:13:43</td>
<td>Interarea</td>
<td>0.000128</td>
</tr>
<tr>
<td>00:13:33</td>
<td>External</td>
<td>0.000075</td>
</tr>
<tr>
<td>00:13:38</td>
<td>NSSA</td>
<td>0.000039</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Cleanup</td>
<td>0.000657</td>
</tr>
</tbody>
</table>

### Last 100 events

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:53</td>
<td>SPF</td>
<td>0.000090</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Stub</td>
<td>0.000041</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Interarea</td>
<td>0.000123</td>
</tr>
<tr>
<td>00:13:53</td>
<td>External</td>
<td>0.000040</td>
</tr>
<tr>
<td>00:13:53</td>
<td>NSSA</td>
<td>0.000038</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Cleanup</td>
<td>0.000657</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Total</td>
<td>0.001252</td>
</tr>
</tbody>
</table>

...
show (ospf | ospf3) neighbor

List of Syntax  Syntax on page 2213
Syntax (EX Series Switches and QFX Series) on page 2213

Syntax

```
show (ospf | ospf3) neighbor
  <brief | detail | extensive>
  <area area-id>
  <instance (all | instance-name)>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
  <neighbor>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

Syntax (EX Series Switches and QFX Series)

```
show (ospf | ospf3) neighbor
  <brief | detail | extensive>
  <area area-id>
  <instance (all | instance-name)>
  <interface interface-name>
  <neighbor>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
instance all option introduced in Junos OS Release 9.1.
instance all option introduced in Junos OS Release 9.1 for EX Series switches.
area, interface, and realm options introduced in Junos OS Release 9.2.
area and interface options introduced in Junos OS Release 9.2 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display information about OSPF neighbors.

CPU utilization might increase while the device learns its OSPF neighbors. We recommend that you use the show (ospf | ospf3) neighbor command after the device learns and establishes OSPF neighbor adjacencies. Depending on the size of your network, this might take several minutes. If you receive a “timeout communicating with routing daemon” error when using the show (ospf | ospf3) neighbor command, wait several minutes before attempting to use the command again. This is not a critical system error, but you might experience a delay in using the CLI.

Options

none—Display standard information about all OSPF neighbors for all routing instances.
brief | detail | extensive—(Optional) Display the specified level of output.
area area-id—(Optional) Display information about the OSPF neighbors for the specified area.
instance (all | instance-name)—(Optional) Display all OSPF interfaces for all routing instances or under the named routing instance.

interface interface-name—(Optional) Display information about OSPF neighbors for the specified logical interface.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor—(Optional) Display information about the specified OSPF neighbor.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display information about the OSPF neighbors for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege**

**Level**

view

**Related Documentation**

- clear (ospf | ospf3) neighbor on page 2158

**List of Sample Output**

- show ospf neighbor brief on page 2216
- show ospf neighbor detail on page 2216
- show ospf neighbor extensive on page 2217
- show ospf neighbor detail on page 2218
- show ospf3 neighbor detail on page 2218
- show ospf neighbor area area-id on page 2218
- show ospf neighbor interface interface-name on page 2218
- show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled) on page 2218

**Output Fields**

Table 161 on page 2214 lists the output fields for the show (ospf | ospf3) neighbor command. Output fields are listed in the approximate order in which they appear.

**Table 161: show (ospf | ospf3) neighbor Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Address of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 161: `show ospf | ospf3 neighbor` 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>State</strong></td>
<td>State of the neighbor:</td>
<td>All levels</td>
</tr>
<tr>
<td>• Attempt—Valid only for neighbors attached to nonbroadcast networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort must be made to contact the neighbor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Down—Initial state of a neighbor conversation. It indicates that no recent information has been received from the neighbor. Hello packets might continue to be sent to neighbors in the Down state, although at a reduced frequency.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Exchange—Routing device is describing its entire link-state database by sending database description packets to the neighbor. Each packet has a sequence number and is explicitly acknowledged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ExStart—First step in creating an adjacency between the two neighboring routing devices. The goal of this step is to determine which routing device is the master, and to determine the initial sequence number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Full—Neighboring routing devices are fully adjacent. These adjacencies appear in router link and network link advertisements.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Init—A hello packet has recently been sent by the neighbor. However, bidirectional communication has not yet been established with the neighbor. This state may occur, for example, because the routing device itself did not appear in the neighbor’s hello packet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Loading—Link-state request packets are sent to the neighbor to acquire more recent advertisements that have been discovered (but not yet received) in the Exchange state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 2Way—Communication between the two routing devices is bidirectional. This state has been ensured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (backup) designated router is selected from the set of neighbors in state 2Way or greater.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Router ID of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Pri</td>
<td>Priority of the neighbor to become the designated router.</td>
<td>All levels</td>
</tr>
<tr>
<td>Dead</td>
<td>Number of seconds until the neighbor becomes unreachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link state acknowledgment list</td>
<td>Number of link-state acknowledgments received.</td>
<td>extensive</td>
</tr>
<tr>
<td>Link state retransmission list</td>
<td>Total number of link-state advertisements retransmitted. For extensive output only, the following information is also displayed:</td>
<td>detail extensive</td>
</tr>
<tr>
<td>• Type—Type of link advertisement: ASBR, Sum, Extern, Network, NSSA, OpaqArea, Router, or Summary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LSA ID—LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Advrtr—Address of the routing device that sent the advertisement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Seq—Link sequence number of the advertisement.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 161: show (ospf | ospf3) neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor-address</td>
<td>(OSPFv3 only) If the neighbor uses virtual links, the Neighbor-address is the site-local, local, or global address. If the neighbor uses a physical interface, the Neighbor-address is an IPv6 link-local address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>area</td>
<td>Area that the neighbor is in.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>OSPF3-Intf-index</td>
<td>(OSPFv3 only) Displays the OSPFv3 interface index.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>opt</td>
<td>Option bits received in the hello packets from the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DR or DR-ID</td>
<td>Address of the designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>BDR or BDR-ID</td>
<td>Address of the backup designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Up</td>
<td>Length of time since the neighbor came up.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>adjacent</td>
<td>Length of time since the adjacency with the neighbor was established.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SPRING Adjacency Labels</td>
<td>Segment routing in networking adjacency labels.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Displayed only when segment routing is enabled</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Segment routing label.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Segment routing flags. Flags VL indicate value and local.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show ospf neighbor brief

```
user@host> show ospf neighbor brief

<table>
<thead>
<tr>
<th>Address</th>
<th>Intf</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.254.225</td>
<td>fxp3.0</td>
<td>2Way</td>
<td>10.250.240.32</td>
<td>128</td>
<td>36</td>
</tr>
<tr>
<td>192.168.254.230</td>
<td>fxp3.0</td>
<td>Full</td>
<td>10.250.240.8</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>192.168.254.229</td>
<td>fxp3.0</td>
<td>Full</td>
<td>10.250.240.35</td>
<td>128</td>
<td>33</td>
</tr>
<tr>
<td>10.1.1.129</td>
<td>fxp2.0</td>
<td>Full</td>
<td>10.250.240.12</td>
<td>128</td>
<td>37</td>
</tr>
<tr>
<td>10.1.1.131</td>
<td>fxp2.0</td>
<td>Full</td>
<td>10.250.240.11</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>10.1.2.1</td>
<td>fxp1.0</td>
<td>Full</td>
<td>10.250.240.9</td>
<td>128</td>
<td>32</td>
</tr>
<tr>
<td>10.1.2.81</td>
<td>fxp0.0</td>
<td>Full</td>
<td>10.250.240.10</td>
<td>128</td>
<td>33</td>
</tr>
</tbody>
</table>
```

show ospf neighbor detail

```
user@host> show ospf neighbor detail

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.6.60</td>
<td>1t-1/2/0.12</td>
<td>Full</td>
<td>1.1.1.60</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>Area 0.0.0.0, opt 0x52, DR 0.0.0.0, BDR 0.0.0.0 Up 23:53:47, adjacent 23:53:34 SPRING Adjacency Labels:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show ospf neighbor extensive

user@host> show ospf neighbor extensive

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.1.2</td>
<td>ge-1/2/0.1</td>
<td>Full</td>
<td>10.5.1.2</td>
<td>128</td>
<td>33</td>
</tr>
<tr>
<td>area 0.0.0.1, opt 0x42, DR 10.5.1.2, BDR 10.5.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up 06:09:42, adjacent 05:17:50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link state retransmission list:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>LSA ID</td>
<td>Adv rtr</td>
<td>Seq</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.56.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.94</td>
<td>10.5.1.94</td>
<td>0x8000005c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>10.5.24.2</td>
<td>10.5.1.94</td>
<td>0x80000036</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.57.0</td>
<td>172.25.27.82</td>
<td>0x80000024</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>1.10.90.0</td>
<td>10.8.1.2</td>
<td>0x80000041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>1.4.109.0</td>
<td>10.6.1.2</td>
<td>0x80000041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.190</td>
<td>10.5.1.190</td>
<td>0x8000005f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>10.5.48.2</td>
<td>10.5.1.190</td>
<td>0x8000003d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.58.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>1.10.91.0</td>
<td>10.8.1.2</td>
<td>0x80000041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>1.4.110.0</td>
<td>10.6.1.2</td>
<td>0x80000041</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.18</td>
<td>10.5.1.18</td>
<td>0x8000005f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>10.5.5.2</td>
<td>10.5.1.18</td>
<td>0x80000033</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.59.0</td>
<td>172.25.27.82</td>
<td>0x8000003a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.62.0</td>
<td>172.25.27.82</td>
<td>0x80000025</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.5.10.2 | ge-1/2/0.10 | ExStart | 10.5.1.38 | 128 | 38 |
| area 0.0.0.1, opt 0x42, DR 10.5.10.2, BDR 10.5.1 |
| Up 06:09:42, master, seq 0xacl530f8, rexmit DBD in 2 sec |
rexmit LSREQ in 0 sec
10.5.11.2  ge-1/2/0.11  Full  10.5.1.42  128  33
area 0.0.0.1, opt 0x42, DR 10.5.11.2, BDR 10.5.11.1
Up 06:09:42, adjacent 05:27:00
Link state retransmission list:

<table>
<thead>
<tr>
<th>Type</th>
<th>LSA ID</th>
<th>Adv rtr</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>10.8.58.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
</tr>
<tr>
<td>Extern</td>
<td>1.10.91.0</td>
<td>10.8.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Extern</td>
<td>1.1.247.0</td>
<td>10.5.1.2</td>
<td>0x8000003f</td>
</tr>
<tr>
<td>Extern</td>
<td>1.4.110.0</td>
<td>10.6.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.18</td>
<td>10.5.1.18</td>
<td>0x80000005f</td>
</tr>
<tr>
<td>Network</td>
<td>10.5.5.2</td>
<td>10.5.1.18</td>
<td>0x80000033</td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.59.0</td>
<td>172.25.27.82</td>
<td>0x80000030</td>
</tr>
</tbody>
</table>

show ospf3 neighbor detail

user@host> show ospf3 neighbor detail

ID               Interface              State     Pri  Dead
10.255.71.13     fe-0/0/2.0             Full      128  30
Neighbor-address fe80::290:69ff:fe9b:e002
area 0.0.0.0, opt 0x13, OSPF3-Intf-Index 2
DR-ID 10.255.71.13, BDR-ID 10.255.71.12
Up 02:51:43, adjacent 02:51:43

show ospf neighbor area area-id

user@host > show ospf neighbor area 1.1.1.1

Address          Interface              State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128  33
Area 1.1.1.1
192.168.37.55    so-1/0/0.0             Full      10.255.245.5     128  37
Area 1.1.1.1

show ospf neighbor interface interface-name

user@host > show ospf neighbor interface so-0/0/0.0

Address          Interface              State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128  33
Area 0.0.0.0
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128  32
Area 1.1.1.1
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128  32
Area 2.2.2.2

show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled)

user @host > show ospf3 neighbor instance all
### Instance: ina

**Realm: ipv6-unicast**

<table>
<thead>
<tr>
<th>ID</th>
<th>Interface</th>
<th>State</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.1.1.1</td>
<td>fe-0/0/2.0</td>
<td>Full</td>
<td>128</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Neighbor-address</td>
<td>fe80::217:cb00:c87c:8c03</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Instance: inb

**Realm: ipv4-unicast**

<table>
<thead>
<tr>
<th>ID</th>
<th>Interface</th>
<th>State</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.1.2.1</td>
<td>fe-0/0/2.1</td>
<td>Full</td>
<td>128</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Neighbor-address</td>
<td>fe80::217:cb00:c97c:8c03</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### show (ospf | ospf3) overview

**List of Syntax**
- Syntax on page 2220
- Syntax (EX Series Switch and QFX Series) on page 2220

**Syntax**
```
show (ospf | ospf3) overview
  <brief | extensive>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

**Syntax (EX Series Switch and QFX Series)**
```
show (ospf | ospf3) overview
  <brief | extensive>
  <instance instance-name>
```

**Release Information**
- Command introduced in Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `realm` option introduced in Junos OS Release 9.2.
- Database protection introduced in Junos 10.2.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**
Display Open Shortest Path First (OSPF) overview information.

**Options**
- **none**—Display standard information about all OSPF neighbors for all routing instances.
- **brief | extensive**—(Optional) Display the specified level of output.
- **instance instance-name**—(Optional) Display all OSPF interfaces under the named routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(Optional) (OSPFv3 only) Display information about the specified OSPFv3 realm, or address family. Use the `realm` option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege Level**
- view

**List of Sample Output**
- show ospf overview (without SRGB) on page 2222
- show ospf overview (with SRGB) on page 2223
- show ospf overview (With Database Protection) on page 2224
- show ospf3 overview (With Database Protection) on page 2224
- show ospf overview extensive on page 2224
**Output Fields**  Table 162 on page 2221 lists the output fields for the `show ospf overview` command. Output fields are listed in the approximate order in which they appear.

**Table 162: show ospf overview Output Fields**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>OSPF routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the routing device.</td>
<td>All levels</td>
</tr>
<tr>
<td>Route table index</td>
<td>Route table index.</td>
<td>All levels</td>
</tr>
<tr>
<td>Configured overload</td>
<td>Overload capability is enabled. If the overload timer is also configured, display the time that remains before it is set to expire. This field is not displayed after the timer expires.</td>
<td>All levels</td>
</tr>
<tr>
<td>Topology</td>
<td>Topology identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Prefix export count</td>
<td>Number of prefixes exported into OSPF.</td>
<td>All levels</td>
</tr>
<tr>
<td>Full SPF runs</td>
<td>Number of complete Shortest Path First calculations.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF delay</td>
<td>Delay before performing consecutive Shortest Path First calculations.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF holdown</td>
<td>Delay before performing additional Shortest Path First (SPF) calculations after the maximum number of consecutive SPF calculations is reached.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF rapid runs</td>
<td>Maximum number of Shortest Path First calculations that can be performed in succession before the hold-down timer begins.</td>
<td>All levels</td>
</tr>
<tr>
<td>LSA refresh time</td>
<td>Refresh period for link-state advertisement (in minutes).</td>
<td>All levels</td>
</tr>
<tr>
<td>SPRING</td>
<td>Source protocol routing in networking: enable or disable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Node Segments</td>
<td>Nodes of source protocol routing in networking: enable or disable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Ipv4 Index</td>
<td>Ipv4 Index.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index Range</td>
<td>Ipv4 Index range.</td>
<td>All levels</td>
</tr>
<tr>
<td>Node Segment Blocks Allocated</td>
<td>Details about node segment blocks.</td>
<td>All levels</td>
</tr>
<tr>
<td>Database protection state</td>
<td>Current state of database protection.</td>
<td>All levels</td>
</tr>
<tr>
<td>Warning threshold</td>
<td>Threshold at which a warning message is logged (percentage of maximum LSA count).</td>
<td>All levels</td>
</tr>
<tr>
<td>Non self-generated LSAs</td>
<td>Number of LSAs whose router ID is not equal to the local router ID: Current, Warning (threshold), and Allowed.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 162: *show ospf overview* Output Fields (continued)

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore time</td>
<td>How long the database has been in the ignore state.</td>
<td>All levels</td>
</tr>
<tr>
<td>Reset time</td>
<td>How long the database must stay out of the ignore or isolated state before it returns to normal operations.</td>
<td>All levels</td>
</tr>
<tr>
<td>Ignore count</td>
<td>Number of times the database has been in the ignore state: <strong>Current</strong> and <strong>Allowed</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart</td>
<td>Graceful restart capability: <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart duration</td>
<td>Time period for complete reacquisition of OSPF neighbors.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart grace period</td>
<td>Time period for which the neighbors should consider the restarting routing device as part of the topology.</td>
<td>All levels</td>
</tr>
<tr>
<td>Graceful restart helper mode</td>
<td>(OSPFv2) Standard graceful restart helper capability (based on RFC 3623): <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart-signaling helper mode</td>
<td>(OSPFv2) Restart signaling-based graceful restart helper capability (based on RFC 4811, RFC 4812, and RFC 4813): <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Helper mode</td>
<td>(OSPFv3) Graceful restart helper capability: <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Trace options</td>
<td>OSPF-specific trace options.</td>
<td>extensive</td>
</tr>
<tr>
<td>Trace file</td>
<td>Name of the file to receive the output of the tracing operation.</td>
<td>extensive</td>
</tr>
<tr>
<td>Area</td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
<tr>
<td>Stub type</td>
<td>Stub type of area: <strong>Normal Stub</strong>, <strong>Not Stub</strong>, or <strong>Not so Stubby Stub</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Type of authentication: <strong>None</strong>, <strong>Password</strong>, or <strong>MD5</strong>.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

**NOTE:** The **Authentication Type** field refers to the authentication configured at the [edit protocols ospf area area-id] level. Any authentication configured for an interface in this area will not affect the value of this field.

| Area border routers         | Number of area border routers.                                                    | All levels      |
| Neighbors                   | Number of autonomous system boundary routers.                                     | All levels      |

**Sample Output**

*show ospf overview (without SRGB)*

```
user@host> show ospf overview
Instance: master
    Router ID: 10.255.245.6
    Route table index: 0
```
show ospf overview (with SRGB)

user@host> show ospf overview

Instance: master
  Router ID: 10.10.10.10
  Route table index: 0
  LSA refresh time: 50 minutes
  Traffic engineering
    SPRING: Enabled
    SRGB Config Range:
      SRGB Start-Label: 1000, SRGB Index-Range: 2000
    SRGB Block Allocation: Success
      SRGB Start Index: 1000, SRGB Size : 2000, Label-Range: [ 1000, 2999 ]
  Node Segments: Enabled
  Ipv4 Index : 1000
  Post Convergence Backup: Disabled
  Area: 0.0.0.0
  Stub type: Not Stub
  Authentication Type: None
  Area border routers: 0, AS boundary routers: 0
  Neighbors
    Up (in full state): 3
  Topology: default (ID 0)
  Prefix export count: 0
  Full SPF runs: 5
  SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
  Backup SPF: Enabled, Remote Backup calculation enabled
### show ospf overview

User@host> `show ospf overview`

- **Instance:** master
- **Router ID:** 10.255.112.218
- **Route table index:** 0
- **LSA refresh time:** 50 minutes
- **Traffic engineering**
- **Restart:** Enabled
  - **Restart duration:** 180 sec
  - **Restart grace period:** 210 sec
  - **Graceful restart helper mode:** Enabled
  - **Restart-signaling helper mode:** Enabled
- **Database protection state:** Normal
- **Warning threshold:** 70 percent
- **Non self-generated LSAs:** Current 582, Warning 700, Allowed 1000
- **Ignore time:** 30, Reset time: 60
- **Ignore count:** Current 0, Allowed 1

**Area:** 0.0.0.0
- **Stub type:** Not Stub
- **Authentication Type:** None
- **Area border routers:** 0, AS boundary routers: 0
- **Neighbors**
  - **Up (in full state):** 160
- **Topology:** default (ID 0)
- **Prefix export count:** 0
- **Full SPF runs:** 70
- **SPF delay:** 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
- **Backup SPF:** Not Needed

### show ospf3 overview

User@host> `show ospf3 overview`

- **Instance:** master
- **Router ID:** 10.255.112.128
- **Route table index:** 0
- **LSA refresh time:** 50 minutes
- **Database protection state:** Normal
- **Warning threshold:** 80 percent
- **Non self-generated LSAs:** Current 3, Warning 8, Allowed 10
- **Ignore time:** 30, Reset time: 60
- **Ignore count:** Current 0, Allowed 2

**Area:** 0.0.0.0
- **Stub type:** Not Stub
- **Area border routers:** 0, AS boundary routers: 0
- **Neighbors**
  - **Up (in full state):** 1
- **Topology:** default (ID 0)
- **Prefix export count:** 0
- **Full SPF runs:** 7
- **SPF delay:** 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
- **Backup SPF:** Not Needed

### show ospf overview extensive

User@host> `show ospf overview extensive`
Instance: master
  Router ID: 1.1.1.103
  Route table index: 0
  Full SPF runs: 13, SPF delay: 0.200000 sec
  LSA refresh time: 50 minutes
  Restart: Disabled
  Trace options: lsa
  Trace file: /var/log/ospf size 131072 files 10
  Area: 0.0.0.0
    Stub type: Not Stub
    Authentication Type: None
    Area border routers: 0, AS boundary routers: 0
  Neighbors
    Up (in full state): 1
show (ospf | ospf3) route

### List of Syntax

Syntax on page 2226
Syntax (EX Series Switch and QFX Series) on page 2226

#### Syntax

- `show (ospf | ospf3) route`
- `<brief | detail | extensive>`
- `<abr | asbr | extern | inter | intra>`
- `<destination>`
- `<instance (default | ipv4-multicast | instance-name)>`
- `<logical-system (default | ipv4-multicast | logical-system-name)>`
- `<network>`
- `<no-backup-coverage>`
- `<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)`
- `<router>`
- `<topology (default | ipv4-multicast | topology-name)`
- `<transit>`

#### Syntax (EX Series Switch and QFX Series)

- `show (ospf | ospf3) route`
- `<brief | detail | extensive>`
- `<abr | asbr | extern | inter | intra>`
- `<destination>`
- `<instance instance-name>`
- `<network>`
- `<no-backup-coverage>`
- `<router>`
- `<topology (default | ipv4-multicast | topology-name)`
- `<transit>`

### Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `topology` option introduced in Junos OS Release 9.0.
- `realm` option introduced in Junos OS Release 9.2.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

### Description

Display the entries in the Open Shortest Path First (OSPF) routing table.

### Options

- `none`—Display standard information about all entries in the OSPF routing table for all routing instances and all topologies.
- `destination`—Display routes to the specified IP address (with optional destination prefix length).
- `brief | detail | extensive`—(Optional) Display the specified level of output.
- `abr`—(Optional) Display routes to area border routers.
- `asbr`—(Optional) Display routes to autonomous system border routers.
extern—(Optional) Display external routes.

inter—(Optional) Display interarea routes.

intra—(Optional) Display intra-area routes.

instance (default | ipv4-multicast | instance-name)—(Optional) Display entries for the default routing instance, the IPv4 multicast routing instance, or for the specified routing instance.

logical-system (default | ipv4-multicast | logical-system-name)—(Optional) Perform this operation on the default logical system, the IPv4 multicast logical system, or on a particular logical system.

network—(Optional) Display routes to networks.

no-backup-coverage—(Optional) Display routes with no backup coverage.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display entries in the routing table for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

router—(Optional) Display routes to all routers.

topology (default | ipv4-multicast | topology-name)—(OSPFv2 only) (Optional) Display routes for the default OSPF topology, IPv4 multicast topology, or for a particular topology.

transit—(Optional) (OSPFv3 only) Display OSPFv3 routes to pseudonodes.

Required Privilege Level

view

List of Sample Output

show ospf route on page 2229
show ospf route detail on page 2230
show ospf route extensive on page 2230
show ospf3 route on page 2230
show ospf3 route detail on page 2231
show ospf3 route topology voice on page 2231

Output Fields

Table 163 on page 2227 list the output fields for the show (ospf | ospf3) route command. Output fields are listed in the approximate order in which they appear.

Table 163: show (ospf | ospf3) route Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Name of the topology.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 163: show (ospf | ospf3) route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Destination of the route.</td>
<td>All levels</td>
</tr>
<tr>
<td>Path type</td>
<td>How the route was learned:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Inter—Interarea route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ext1—External type 1 route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ext2—External type 2 route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• intra—Intra-area route</td>
<td></td>
</tr>
<tr>
<td>Route type</td>
<td>The type of routing device from which the route was learned:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• AS BR—Route to AS border router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Area BR—Route to area border router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Area/AS BR—Route to router that is both an Area BR and AS BR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network—Network router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Router—Route to a router that is neither an Area BR nor an AS BR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transit—(OSPFv3 only) Route to a pseudonode representing a transit network, LAN, or nonbroadcast multiaccess (NBMA) link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discard—Route to a summary discard.</td>
<td></td>
</tr>
<tr>
<td>NH Type</td>
<td>Next-hop type: LSP or IP.</td>
<td>All levels</td>
</tr>
<tr>
<td>Metric</td>
<td>Route's metric value.</td>
<td>All levels</td>
</tr>
<tr>
<td>NH-interface</td>
<td>(OSPFv3 only) Interface through which the route's next hop is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>NH-addr</td>
<td>(OSPFv3 only) IPv6 address of the next hop.</td>
<td>All levels</td>
</tr>
<tr>
<td>NextHop Interface</td>
<td>(OSPFv2 only) Interface through which the route's next hop is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nexthop addr/label</td>
<td>(OSPFv2 only) If the NH Type is IP, then it is the address of the next hop. If the NH Type is LSP, then it is the name of the label-switched path.</td>
<td>All levels</td>
</tr>
<tr>
<td>Area</td>
<td>Area ID of the route.</td>
<td>detail</td>
</tr>
<tr>
<td>Origin</td>
<td>Router from which the route was learned.</td>
<td>detail</td>
</tr>
<tr>
<td>Type 7</td>
<td>Route was learned through a not-so-stubby area (NSSA) link-state advertisement (LSA).</td>
<td>detail</td>
</tr>
<tr>
<td>P-bit</td>
<td>Route was learned through NSSA LSA and the propagate bit was set.</td>
<td>detail</td>
</tr>
<tr>
<td>Fwd NZ</td>
<td>Forwarding address is nonzero. Fwd NZ is only displayed if the route is learned through an NSSA LSA.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 163: show (ospf | ospf3) route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>optional-capability</td>
<td>Optional capabilities propagated in the router LSA. This field is in the output for intra-area router routes only (when Route Type is Area BR, AS BR, Area/AS BR, or Router), not for interarea router routes or network routes. Three bits in this field are defined as follows:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 0x4 (V)—Routing device is at the end of a virtual active link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x2 (E)—Routing device is an autonomous system boundary router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 (B)—Routing device is an area border router.</td>
<td></td>
</tr>
<tr>
<td>priority</td>
<td>The priority assigned to the prefix:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• high</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• low</td>
<td></td>
</tr>
<tr>
<td>NOTE:</td>
<td>The priority field applies only to routes of type Network.</td>
<td></td>
</tr>
<tr>
<td>BGP-ORR Generation-ID</td>
<td>Display the BGP-ORR generation identifier of the main OSPF route. This field is shown only for non-zero values.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show ospf route

```
user@host> show ospf route

Topology default Route Table:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path Type</th>
<th>Route Type</th>
<th>NH Type</th>
<th>Metric</th>
<th>NextHop</th>
<th>NextHop Address/LSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.60/32</td>
<td>Intra Network</td>
<td>Spring Bkup</td>
<td>lt-1/2/0.14</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1.70/32</td>
<td>Intra Network</td>
<td>IP Bkup LSP</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70 (null)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1.80/32</td>
<td>Intra Network</td>
<td>IP Bkup IP</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802068 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.14</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802078 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.14</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802088 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802098 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802108 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802118 (S=0)</td>
<td>Intra Network</td>
<td>Mpls Bkup MPLS</td>
<td>lt-1/2/0.12</td>
<td>10.0.10.70</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show ospf route detail

```
user@host> show ospf route detail
Topology default Route Table:
Prefix      Path    Route      NH   Metric  NextHop       Nexthop
Type       Type    Type        Interface     addr/label
10.255.14.174 Inter AS BR IP       210 t1-3/0/1.0
area 0.0.0.2, origin 10.255.14.185
10.255.14.178 Intra Router IP      200 t3-3/1/3.0
area 0.0.0.2, origin 10.255.14.178, optional-capability 0x0
10.210.1.0/30  Inter Network IP     10 t3-3/1/2.0
area 0.0.0.2, origin 10.255.14.172, priority medium
198.51.100/24  Inter Network IP     210 t1-3/0/1.0
area 0.0.0.2, origin 10.255.14.185, priority low
192.0.2.0/24 Ext2 Network IP       0 t3-3/0/1.0
area 0.0.0.0, origin 10.255.14.174, priority high
203.3.113.0/24 Inter Network IP     220 t3-3/0/1.0
area 0.0.0.2, origin 10.255.14.185, priority high
```

show ospf route extensive

```
user@host> show ospf route extensive
Topology default Route Table:
Prefix      Path    Route      NH   Metric  NextHop       Nexthop
Type       Type    Type        Interface     Address/LSP
1.1.1.1      Intra Router IP      100 ge-0/0/2.0
area 0.0.0.0, origin 1.1.1.1, optional-capability 0x0
1.1.1.1/32   Inter Network IP     100 ge-0/0/2.0
area 0.0.0.0, origin 1.1.1.1, priority medium
BGP-ORR generation-id: 1
```

show ospf3 route

```
user@host> show ospf3 route
Prefix      Path    Route      NH   Metric  NextHop       Nexthop
Type       Type    Type        Interface     addr/label
10.255.71.13 Inter Router IP      1
NH-interface fe-0/0/2.0, NH-addr fe80::290:69ff:fe9b:e002
10.255.71.13/0.0.0.2
10.255.245.1 Intra Router IP      40 fxp1.1
area 0.0.0.0, origin 10.255.245.1, optional-capability 0x0,
192.168.36.17
10.255.245.3 Intra AS BR IP       1 fxp2.3
area 0.0.0.0, origin 10.255.245.3, optional-capability 0x0,
192.168.36.34
10.255.245.1/32  Inter Network IP     40 fxp1.1
area 0.0.0.0, origin 10.255.245.1, priority high
192.168.36.17
10.255.245.2/32 Intra Network IP     0 lo0.0
area 0.0.0.0, origin 10.255.245.2, priority medium
```

Copyright © 2019, Juniper Networks, Inc.
show ospf3 route detail

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path type</th>
<th>Route type</th>
<th>NH type</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.174</td>
<td>Intra</td>
<td>Area/AS BR</td>
<td>IP</td>
<td>110</td>
</tr>
<tr>
<td>10.255.14.178</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>200</td>
</tr>
<tr>
<td>10.255.14.185;0.0.0.2</td>
<td>Intra</td>
<td>Transit</td>
<td>IP</td>
<td>200</td>
</tr>
<tr>
<td>1000:1:1::1/128</td>
<td>Inter</td>
<td>Network</td>
<td>IP</td>
<td>110</td>
</tr>
<tr>
<td>1001:2:1::/48</td>
<td>Ext1</td>
<td>Network</td>
<td>IP</td>
<td>110</td>
</tr>
<tr>
<td>1002:1:7::/48</td>
<td>Ext2</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
</tr>
<tr>
<td>1002:3:4::/48</td>
<td>Ext2</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
</tr>
<tr>
<td>abcd::71:12/128</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
</tr>
<tr>
<td>abcd::71:13/128</td>
<td>Intra</td>
<td>LSP</td>
<td>IP</td>
<td>1</td>
</tr>
</tbody>
</table>

show ospf route topology voice

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path Type</th>
<th>Route Type</th>
<th>NH Metric</th>
<th>NextHop Interface</th>
<th>NextHop addr/label</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.8.2</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>0</td>
</tr>
<tr>
<td>10.255.8.3</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>0</td>
</tr>
<tr>
<td>10.255.8.1/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>10.255.8.2/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>10.255.8.3/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>192.168.8.0/29</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>192.168.8.44/30</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>192.168.8.46/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>so-0/2/0.0</td>
<td>lo0.0</td>
</tr>
<tr>
<td>IP Address</td>
<td>Network</td>
<td>Interface</td>
<td>status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>------------</td>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.8.48/30</td>
<td>Intra Network</td>
<td>IP 1</td>
<td>so-0/2/1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.8.52/30</td>
<td>Intra Network</td>
<td>IP 2</td>
<td>so-0/2/0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.9.44/30</td>
<td>Intra Network</td>
<td>IP 1</td>
<td>so-0/2/0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.9.45/32</td>
<td>Intra Network</td>
<td>IP 2</td>
<td>so-0/2/0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show (ospf | ospf3) statistics

List of Syntax  
Syntax on page 2233  
Syntax (EX Series Switch and QFX Series) on page 2233

Syntax  
```
show (ospf | ospf3) statistics
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

Syntax (EX Series Switch and QFX Series)  
```
show (ospf | ospf3) statistics
  <instance instance-name>
```

Release Information  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
realm option introduced in Junos OS Release 9.2.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  
Display OSPF statistics.

Options  
none—Display OSPF statistics for all routing instances.

  instance instance-name—(Optional) Display all statistics for the specified routing instance.

  logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

  realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Display all statistics for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege  
view

Related Documentation  
• clear (ospf | ospf3) statistics on page 2161

List of Sample Output  
show ospf statistics on page 2235  
show ospf statistics logical-system all on page 2235  
show ospf3 statistics on page 2236

Output Fields  
Table 164 on page 2234 lists the output fields for the show (ospf | ospf3) statistics command. Output fields are listed in the approximate order in which they appear.
Table 164: show (ospf | ospf3) statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet type</td>
<td>Type of OSPF packet.</td>
</tr>
<tr>
<td>Total Sent/Total Received</td>
<td>Total number of packets sent and received.</td>
</tr>
<tr>
<td>Last 5 seconds Sent/Last 5 seconds Received</td>
<td>Total number of packets sent and received in the last 5 seconds.</td>
</tr>
<tr>
<td>DBDs retransmitted</td>
<td>Total number of database description packets retransmitted, and number retransmitted in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs flooded</td>
<td>Total number of link-state advertisements flooded, and number flooded in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs flooded high-prio</td>
<td>Total number of high priority link-state advertisements flooded, and number flooded in the last 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>A link-state advertisement is deemed a high priority if it has changed since it was last sent.</td>
</tr>
<tr>
<td>LSAs retransmitted</td>
<td>Total number of link-state advertisements retransmitted, and number retransmitted in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs transmitted to nbr</td>
<td>Total number of link-state advertisements transmitted to a neighbor, and number transmitted in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs requested</td>
<td>Total number of link-state advertisements requested by neighboring devices, and number requested in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs acknowledged</td>
<td>Total number of link-state advertisements acknowledged, and number acknowledged in the last 5 seconds.</td>
</tr>
<tr>
<td>Flood queue depth</td>
<td>Total number of entries in the extended queue.</td>
</tr>
<tr>
<td>Total rexmit entries</td>
<td>Total number of retransmission entries waiting to be sent from the OSPF routing instance.</td>
</tr>
<tr>
<td>db summaries</td>
<td>Total number of database description summaries waiting to be sent from the OSPF routing instance.</td>
</tr>
<tr>
<td>Isreq entries</td>
<td>Total number of link-state request entries waiting to be sent from the OSPF routing instance.</td>
</tr>
</tbody>
</table>
### Table 164: `show (ospf | ospf3) statistics` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive errors</td>
<td>Number and type of receive errors. Some sample receive errors include:</td>
</tr>
<tr>
<td></td>
<td>• mtu mismatches</td>
</tr>
<tr>
<td></td>
<td>• no interface found</td>
</tr>
<tr>
<td></td>
<td>• no virtual link found</td>
</tr>
<tr>
<td></td>
<td>• nssa mismatches</td>
</tr>
<tr>
<td></td>
<td>• stub area mismatches</td>
</tr>
<tr>
<td></td>
<td>• subnet mismatches</td>
</tr>
</tbody>
</table>

If there are no receive errors, the output displays **none**.

### Sample Output

**show ospf statistics**

```
user@host> show ospf statistics

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Hello</td>
<td>31</td>
<td>14</td>
</tr>
<tr>
<td>DbD</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>LSReq</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>LSUpdate</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>LSAck</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

DBDs retransmitted : 3, last 5 seconds : 0
LSAs flooded : 12, last 5 seconds : 0
LSAs flooded high-prio : 0, last 5 seconds : 0
LSAs retransmitted : 0, last 5 seconds : 0
LSAs transmitted to nbr: 3, last 5 seconds : 0
LSAs requested : 5, last 5 seconds : 0
LSAs acknowledged : 19, last 5 seconds : 0

Flood queue depth : 0
Total rexmit entries : 0
db summaries : 0
lsreq entries : 0

Receive errors:
862 no interface found
115923 no virtual link found
```

**show ospf statistics logical-system all**

```
user@host> show ospf statistics logical-system all

logical-system: C
OSPF instance is not running
-----

logical-system: B
```
### show ospf3 statistics

#### logical-system: A

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total Sent</th>
<th>Total Received</th>
<th>Last 5 seconds Sent</th>
<th>Last 5 seconds Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>313740</td>
<td>313653</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>DbD</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSReq</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSU</td>
<td>2752</td>
<td>1825</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSACK</td>
<td>1821</td>
<td>2747</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

DBDs retransmitted 0, last 5 seconds 0
LSAs flooded 2741, last 5 seconds 0
LSAs flooded high-prio 10, last 5 seconds 0
LSAs retransmitted 0, last 5 seconds 0
LSAs transmitted to nbr 2, last 5 seconds 0
LSAs requested 1, last 5 seconds 0
LSAs acknowledged 1831, last 5 seconds 0

Flood queue depth 0
Total rexmit entries 0
db summaries 0
lsreq entries 0

Receive errors:
None

-----

### show ospf3 statistics

#### logical-system: A

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total Sent</th>
<th>Total Received</th>
<th>Last 5 seconds Sent</th>
<th>Last 5 seconds Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DbD</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

DBDs retransmitted 0, last 5 seconds 0
LSAs flooded 1825, last 5 seconds 0
LSAs flooded high-prio 10, last 5 seconds 0
LSAs retransmitted 0, last 5 seconds 0
LSAs transmitted to nbr 1, last 5 seconds 0
LSAs requested 2, last 5 seconds 0
LSAs acknowledged 2748, last 5 seconds 0

Flood queue depth 0
Total rexmit entries 0
db summaries 0
lsreq entries 0

Receive errors:
None

-----
<table>
<thead>
<tr>
<th>LSReq</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSUpdate</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSAck</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DBDs retransmitted</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs flooded</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs flooded high-prio</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs retransmitted</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs transmitted to nbr:</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs requested</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSAs acknowledged</td>
<td>0, last 5 seconds : 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood queue depth</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total rexmit entries</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db summaries</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lsreq entries</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Receive errors:
- None
CHAPTER 25

Protocol-Independent Routing Operational Commands

- show as-path
- show as-path domain
- show as-path summary
- show route
- show route active-path
- show route advertising-protocol
- show route all
- show route aspath-regex
- show route best
- show route brief
- show route ccc
- show route community
- show route community-name
- show route damping
- show route detail
- show route exact
- show route export
- show route export vrf-target
- show route extensive
- show route flow validation
- show route forwarding-table
- show route forwarding-table interface-name
- show route hidden
- show route inactive-path
- show route inactive-prefix
- show route instance
- show route label
- show route label-switched-path
- show route localization
- show route martians
- show route match-prefix
- show route next-hop
- show route no-community
- show route output
- show route protocol
- show route range
- show route receive-protocol
- show route resolution
- show route snooping
- show route source-gateway
- show route summary
- show route table
- show route terse
show as-path

List of Syntax  Syntax on page 2241
Syntax (EX Series Switches) on page 2241

Syntax  show as-path
       <brief | detail>
       <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show as-path
       <brief | detail>

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Display the distribution of autonomous system (AS) paths that the local routing device
is using (usually through the routing table). Use this command to debug problems for
AS paths and to understand how AS paths have been manipulated through a policy
(through the as-path-prepend action) or through aggregation.

AS paths are stored in a hash table. A hash table is one method for fast lookup. Each
entry in the table is called a bucket. Junos OS computes a hash value that indicates in
which bucket the AS path is stored. The AS paths are dispersed among the hash buckets
so that a manageable number of AS paths is stored in each bucket. Only unique AS paths
are stored. Duplicate AS paths increase a reference count, but do not increase the number
of AS paths stored in the hash table.

Options  none—Display basic information about AS paths that the local routing device is using
(same as brief).

brief | detail—(Optional) Display the specified level of output.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all
logical systems or on a particular logical system.

Required Privilege Level  view

Related Documentation  • show as-path summary on page 2249

List of Sample Output  show as-path on page 2242
show as-path detail on page 2243
Output Fields  

Table 165 on page 2242 lists the output fields for the show as-path command. Output fields are listed in the approximate order in which they appear.

**Table 165: show as-path Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total AS paths</td>
<td>Total number of AS paths.</td>
<td>brief none</td>
</tr>
<tr>
<td>Bucket</td>
<td>Bucket number.</td>
<td>All levels</td>
</tr>
<tr>
<td>Count</td>
<td>Number of AS path entries in this bucket.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
| **AS path** | 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:  
  - I—IGP.  
  - E—EGP.  
  - ?—Incomplete; typically, the AS path was aggregated.  
  - Atomic—Route is an aggregate of several route prefixes.  
  - Aggregator—Routing device has summarized a range of prefixes. | All levels |
| domain | Number of independent AS domains. The AS paths of an independent AS domain are not shared with the AS paths and AS path attributes of other domains, including the master routing instance domain. | detail |
| neighbor as | AS peer address. | detail |
| length | Length of the AS path. | detail |
| segments | Length of the AS segment descriptor. | detail |
| unique-count | Number of unique autonomous systems (ASs) present in the AS path | detail |
| references | Path reference count. | detail |

**Sample Output**

**show as-path**

```
user@host> show as-path
Total AS paths: 30382
Bucket Count: 36
  I
  14203 2914 174 31752 I
  14203 2914 701 21512 I
  14203 2914 1239 26632 I
  14203 2914 1239 29704 I
  14203 2914 4323 10248 I
  14203 2914 4766 23560 I
  14203 2914 6395 32776 I
  14203 2914 7911 11272 I
```
show as-path detail

user@host> show as-path detail
Total AS paths: 30410
Bucket 0  Count: 36
  AS path: I
    domain 0, length 0, segments 0, unique-count 0, references 54
  AS path: 14203 2914 174 31752 I
    domain 1, neighbor as: 14203, length 4, segments 1, unique-count 4,
    references 2
  AS path: 14203 2914 701 21512 I
    domain 1, neighbor as: 14203, length 4, segments 1, unique-count 4,
    references 2
  AS path: 14203 2914 1239 26632 I
    domain 1, neighbor as: 14203, length 4, segments 1, unique-count 5,
    references 2
  AS path: 14203 2914 1239 29704 I
    domain 1, neighbor as: 14203, length 4, segments 1, unique-count 4,
    references 2
  AS path: 14203 2914 4323 10248 I
    domain 1, neighbor as: 14203, length 4, segments 1, unique-count 6,
references 2
   AS path: 14203 2914 7911 14325 14325 14348 I
      domain 1, neighbor as: 14203, length 6, segments 1, unique-count 4,
      references 2
   AS path: 14203 2914 701 4637 9230 9230 9230 I
      domain 1, neighbor as: 14203, length 7, segments 1, unique-count 4,
      references 3
   AS path: 14203 2914 6395 14 14 14 14 I
      domain 1, neighbor as: 14203, length 7, segments 1, unique-count 4,
      references 10
...
**show as-path domain**

**List of Syntax**  
Syntax on page 2246  
Syntax (EX Series Switches) on page 2246

**Syntax**  
```text
show as-path domain  
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**  
```text
show as-path domain
```

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

**Description**  
Display autonomous system (AS) path domain information.

**Options**  
```text
none—(Optional) Display AS path domain information for all routing instances.  
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 as-path domain on page 2248`

**Output Fields**  
`Table 166 on page 2246 lists the output fields for the show as-path domain command. Output fields are listed in the approximate order in which they appear`

**Table 166: show as-path domain Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Number of independent AS domains. The AS paths of an independent AS domain are not shared with the AS paths and AS path attributes of other domains, including the master routing instance domain.</td>
</tr>
<tr>
<td>Primary</td>
<td>Primary AS number.</td>
</tr>
<tr>
<td>References</td>
<td>Path reference count.</td>
</tr>
<tr>
<td>Number Paths</td>
<td>Number of known AS paths.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the AS path:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ASLoop</strong>—Path contains an AS loop.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Atomic</strong>—Path includes the ATOMIC_AGGREGATE path attribute.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local</strong>—Path was created by local aggregation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Master</strong>—Path was created by the master routing instance.</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>AS number of the local routing device.</td>
</tr>
<tr>
<td><strong>Loops</strong></td>
<td>How many times this AS number can appear in an AS path.</td>
</tr>
</tbody>
</table>
### Sample Output

```
show as-path domain
```

<table>
<thead>
<tr>
<th>Domain: 1</th>
<th>Primary: 10458</th>
</tr>
</thead>
<tbody>
<tr>
<td>References:</td>
<td>3 Paths: 30383</td>
</tr>
<tr>
<td>Flags: Master</td>
<td></td>
</tr>
<tr>
<td>Local AS: 10458</td>
<td>Loops: 1</td>
</tr>
</tbody>
</table>

---

Interfaces Fundamentals for Routing Devices
show as-path summary

List of Syntax  Syntax on page 2249
Syntax (EX Series Switches) on page 2249

Syntax  show as-path summary
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show as-path summary

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

Description  Display autonomous system (AS) path summary information.

AS paths are stored in a hash table. A hash table is one method for fast lookup. Each
entry in the table is called a bucket. Junos OS computes a hash value that indicates in
which bucket the AS path is stored. The AS paths are dispersed among the hash buckets
so that a manageable number of AS paths is stored in each bucket. Only unique AS paths
are stored. Duplicate AS paths increase a reference count, but do not increase the number
of AS paths stored in the hash table.

Options  none—(Optional) Display AS path summary information for all routing instances.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all
logical systems or on a particular logical system.

Required Privilege  view

Related Documentation  •  show as-path on page 2241

List of Sample Output  show as-path summary on page 2250

Output Fields  Table 167 on page 2249 lists the output fields for the show as-path summary command.
Output fields are listed in the approximate order in which they appear.

Table 167: show as-path summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Paths</td>
<td>Number of AS paths.</td>
</tr>
<tr>
<td>Buckets</td>
<td>Number of hash buckets in use.</td>
</tr>
</tbody>
</table>
Table 167: show as-path summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max</td>
<td>Maximum number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Min</td>
<td>Minimum number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Avg</td>
<td>Average number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Std deviation</td>
<td>Standard deviation of AS path entries per bucket.</td>
</tr>
</tbody>
</table>

Sample Output

**show as-path summary**

```
user@host> show as-path summary

<table>
<thead>
<tr>
<th>AS Paths</th>
<th>Buckets</th>
<th>Max</th>
<th>Min</th>
<th>Avg</th>
<th>Std deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>30425</td>
<td>1024</td>
<td>95</td>
<td>12</td>
<td>29</td>
<td>6.481419</td>
</tr>
</tbody>
</table>
```
show route

List of Syntax  Syntax on page 2251
Syntax (EX Series Switches) on page 2251

Syntax  
show route
<all>
<destination-prefix>
<logical-system (all | logical-system-name)>
<private>
<te-ipv4-prefix-ip te-ipv4-prefix-ip>
<te-ipv4-prefix-node-ip te-ipv4-prefix-node-ip>
<te-ipv4-prefix-node-iso te-ipv4-prefix-node-iso>

Syntax (EX Series Switches)  
show route
<all>
<destination-prefix>
<private>

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option private introduced in Junos OS Release 9.5.
Option private introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 15.1R3 on MX Series routers for enhanced subscriber management.
Options te-ipv4-prefix-ip, te-ipv4-prefix-node-ip, and te-ipv4-prefix-node-iso introduced in Junos OS Release 17.2R1 on MX Series and PTX Series.

Description  
Display the active entries in the routing tables.

Options  
none—Display brief information about all active entries in the routing tables.

all—(Optional) Display information about all routing tables, including private, or internal, routing tables.

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.

private—(Optional) Display information only about all private, or internal, routing tables.

display-client-data—(Optional) Display client id and cookie information for routes installed by the routing protocol process client applications.
te-ipv4-prefix-ip  te-ipv4-prefix-ip—(Optional) Display IPv4 address of the traffic-engineering prefix, without the mask length if present in the routing table.

te-ipv4-prefix-node-ip  te-ipv4-prefix-node-ip—(Optional) Display all prefixes that have originated from the traffic-engineering node. You can filter IPv4 node addresses from the traffic-engineered routes in the Isdist.0 table.

te-ipv4-prefix-node-iso  te-ipv4-prefix-node-iso—(Optional) Display all prefixes that have originated from the traffic-engineering node. You can filter IPv4 routes with the specified ISO circuit ID from the Isdist.0 table.

Required Privilege
Level

view

Related Documentation

• Understanding IS-IS Configuration
  • Example: Configuring IS-IS
  • Examples: Configuring Internal BGP Peering
  • Examples: Configuring External BGP Peering
  • Examples: Configuring OSPF Routing Policy
  • Verifying and Managing Junos OS Enhanced Subscriber Management

List of Sample Output

show route on page 2255
show route (VPN) on page 2256
show route (with Destination Prefix) on page 2256
show route destination-prefix detail on page 2256
show route extensive on page 2256
show route extensive (ECMP) on page 2257
show route extensive (Multipath Resolution) on page 2257
show route (Enhanced Subscriber Management) on page 2262
show route (IPv6 Flow Specification) on page 2262
show route display-client-data detail on page 2262
show route te-ipv4-prefix-ip on page 2263
show route te-ipv4-prefix-ip extensive on page 2264
show route te-ipv4-prefix-node-iso on page 2266
show route te-ipv4-prefix-node-iso extensive on page 2267
show route te-ipv4-prefix-node-iso detail on page 2269

Output Fields

Table 168 on page 2252 describes the output fields for the show route command. Output fields are listed in the approximate order in which they appear.

Table 168: show route 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>
</tbody>
</table>
Table 168: show route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active).</td>
</tr>
<tr>
<td></td>
<td>• holdown (routes that are in the pending state before being declared inactive). A holdown route</td>
</tr>
<tr>
<td></td>
<td>was once the active route and is no longer the active route. The route is in the holdown state</td>
</tr>
<tr>
<td></td>
<td>because a protocol still has interest in the route, meaning that the interest bit is set. A</td>
</tr>
<tr>
<td></td>
<td>protocol might have its interest bit set on the previously active route because the protocol is</td>
</tr>
<tr>
<td></td>
<td>still advertising the route. The route will be deleted after all protocols withdraw their</td>
</tr>
<tr>
<td></td>
<td>advertisement of the route and remove their interest bit. A persistent holdown state often means</td>
</tr>
<tr>
<td></td>
<td>that the interested protocol is not releasing its interest bit properly.</td>
</tr>
<tr>
<td></td>
<td>However, if you have configured advertisement of multiple routes (with the add-path or</td>
</tr>
<tr>
<td></td>
<td>advertise-inactive statement), the holdown bit is most likely set because BGP is advertising the</td>
</tr>
<tr>
<td></td>
<td>route as an active route. In this case, you can ignore the holdown state because nothing is wrong.</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy).</td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Route destination (for example: 10.0.0.1/24). Sometimes the route information is presented in another</td>
</tr>
<tr>
<td></td>
<td>format, such as:</td>
</tr>
<tr>
<td></td>
<td>• MPLS-label (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• interface-name (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only. For</td>
</tr>
<tr>
<td></td>
<td>example, 10.11.195:NoCtrlWord:1:1:Local/96):</td>
</tr>
<tr>
<td></td>
<td>• neighbor-address—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• control-word-status—Whether the use of the control word has been negotiated for this virtual</td>
</tr>
<tr>
<td></td>
<td>circuit: NoCtrlWord or CtrlWord.</td>
</tr>
<tr>
<td></td>
<td>• encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2)</td>
</tr>
<tr>
<td></td>
<td>ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet,</td>
</tr>
<tr>
<td></td>
<td>(6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.</td>
</tr>
<tr>
<td></td>
<td>• vc-id—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>• source—Source of the advertisement: Local or Remote.</td>
</tr>
<tr>
<td>protocol, preference</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into</td>
</tr>
<tr>
<td></td>
<td>the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• −—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• *—An asterisk indicates that the route is both the active and the last active route. An asterisk</td>
</tr>
<tr>
<td></td>
<td>before a to line indicates the best subpath to the route.</td>
</tr>
</tbody>
</table>

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.

| weeks:days hours:minutes:seconds | How long the route been known (for example, 2w4d 13:11:14, or 2 weeks, 4 days, 13 hours, 11 minutes, and 14 seconds). |
### Table 168: show route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by the 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>localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>from</td>
<td>Interface from which the route was received.</td>
</tr>
</tbody>
</table>
| AS path    | 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:  
- I—IGP.  
- E—EGP.  
- ?—Incomplete; typically, the AS path was aggregated.  
When AS path numbers are included in the route, the format is as follows:  
- [ ]—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.  
- { }—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.  
- ( )—Parentheses enclose a confederation.  
- ( [ ] )—Parentheses and brackets enclose a confederation set.  
**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance. |
| encapsulated | Extended next-hop encoding capability enabled for the specified BGP community for routing IPv4 traffic over IPv6 tunnels. When BGP receives routes without the tunnel community, IPv4-Over IPv6 tunnels are not created and BGP routes are resolved without encapsulation. |
| Route Labels | Stack of labels carried in the BGP route update. |
| validation-state | (BGP-learned routes) Validation status of the route:  
- 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.  
- Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database.  
- Unverified—Indicates that the origin of the prefix is not verified against the database. This is because the database got populated and the validation is not called for in the BGP import policy, although origin validation is enabled, or the origin validation is not enabled for the BGP peers.  
- Valid—Indicates that the prefix and autonomous system pair are found in the database. |
| to          | Next hop to the destination. An angle bracket (>) indicates that the route is the selected route.  
If the destination is Discard, traffic is dropped. |
### Table 168: show route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>via</strong></td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word <strong>Selected</strong>. This field can also contain the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weight</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Balance</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>lsp-path-name</strong>—Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td></td>
<td>• <strong>label-action</strong>—MPLS label and operation occurring at the next hop. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label). For VPNs, expect to see multiple <strong>push</strong> operations, corresponding to the inner and outer labels required for VPN routes (in the case of a direct PE-to-PE connection, the VPN route would have the inner label push only).</td>
</tr>
</tbody>
</table>

#### Private unicast

(Enhanced subscriber management for MX Series routers) Indicates that an access-internal route is managed by enhanced subscriber management. By contrast, access-internal routes not managed by enhanced subscriber management are displayed with associated next-hop and media access control (MAC) address information.

#### balance

Distribution of the load based on the underlying operational interface bandwidth for equal-cost multipaths (ECMP) across the next-hop gateways in percentages.

### Sample Output

**show route**

```
user@host> show route

inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:65500:1:10.0.0.20/240
  *[MVPN/70] 19:53:41, metric 2
  Indirect

1:65500:1:10.0.0.40/240
  *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
  AS path: I
  > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD
  [BGP/170] 19:53:26, localpref 100, from 10.0.0.33
  AS path: I
  > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD

1:65500:1:10.0.0.60/240
  *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
  AS path: I
  > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF
  [BGP/170] 19:53:25, localpref 100, from 10.0.0.33
  AS path: I
  > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toF
```
show route (VPN)

The following sample output shows a VPN route with composite next hops enabled. The first Push operation corresponds to the outer label. The second Push operation corresponds to the inner label.

```
user@host> show route 192.0.2.0

13979:665001.inet.0: 871 destinations, 3556 routes (871 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.0.2.0/24        [BGP/170] 00:28:32, localpref 100, from 10.9.9.160
                        AS path: 13980 ?, validation-state: unverified
                        > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
                        [BGP/170] 00:28:28, localpref 100, from 10.9.9.169
                        AS path: 13980 ?, validation-state: unverified
                        > to 10.100.0.42 via ae2.0, Push 126016, Push 300368(top)
                        #[Multipath/255] 00:28:28, metric2 102
                        > to 10.100.0.42 via ae2.0, Push 16, Push 300368(top)
```

show route (with Destination Prefix)

```
user@host> show route 192.168.0.0/12

inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/12      *[Static/5] 2w4d 12:54:27
                        > to 192.168.167.254 via fxp0.0
```

show route destination-prefix detail

```
user@host> show route 198.51.100.0 detail

inet.0: 15 destinations, 20 routes (15 active, 0 holddown, 0 hidden)
198.51.100.0/24 (2 entries, 2 announced)
*BGP    Preference: 170/-101
... BGP-Static Preference: 4294967292
    Next hop type: Discard
    Address: 0x9041ae4
    Next-hop reference count: 2
    State: <NoReadvrt Int Ext AlwaysFlash>
    Inactive reason: Route Preference
    Local AS:   200
    Age: 4d 1:40:40
    Validation State: unverified
    Task: RT
    Announcement bits (1): 2-BGP_RT_Background
    AS path: 4 5 6 I
```

show route extensive

```
user@host> show route extensive
```
v1.mvpn.0: 5 destinations, 8 routes (5 active, 1 holddown, 0 hidden)
1:65500:1:10.0.0.40/240 (1 entry, 1 announced)
  *BGP Preference: 170/-101
  PMSI: Flags 0x0: Label[0:0:0]: PIM-SM: Sender 10.0.0.40 Group

203.0.113.1
  Next hop type: Indirect
  Address: 0x92455b8
  Next-hop reference count: 2
  Source: 10.0.0.30
  Protocol next hop: 10.0.0.40
  Indirect next hop: 2 no-forward
  State: <Active Int Ext>
    Local AS: 64510 Peer AS: 64511
    Age: 3 Metric2: 1
    Validation State: unverified
    Task: BGP_64510.10.0.0.30+179
    Announcement bits (2): 0-PIM.v1 1-mvpn global task
    AS path: I (Originator) Cluster list: 10.0.0.30
    AS path: Originator ID: 10.0.0.40
    Communities: target:64502:100 encapsulation:0L:14
    Import Accepted
    Localpref: 100
    Router ID: 10.0.0.30
    Primary Routing Table bgp.mvpn.0
  Indirect next hops: 1
    Protocol next hop: 10.0.0.40 Metric: 1
    Indirect next hop: 2 no-forward
    Indirect path forwarding next hops: 1
      Next hop type: Router
      Next hop: 10.0.24.4 via lt-0/3/0.24 weight 0x1
    10.0.0.40/32 Originating RIB: inet.3
    Metric: 1 Node path count: 1
    Forwarding nexthops: 1
      Nexthop: 10.0.24.4 via lt-0/3/0.24

show route extensive (ECMP)

user@host> show route extensive

  *IS-IS Preference: 15
    Level: 1
    Next hop type: Router, Next hop index: 1048577
    Address: 0xXXXXXXXXXX
    Next-hop reference count: YY
    Next hop: 198.51.100.2 via ae1.0 balance 43%, selected
    Session Id: 0x141
    Next hop: 192.0.2.2 via ae0.0 balance 57%

show route extensive (Multipath Resolution)

user@host> show route extensive

inet.0: 37 destinations, 37 routes (36 active, 0 holddown, 1 hidden)
10.1.1.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.1.1.2/32 -> {indirect(1048574)}
  *Static Preference: 5
  Next hop type: Indirect, Next hop index: 0
  Address: 0xb39d1b0
Next-hop reference count: 2
Next hop type: Router, Next hop index: 581
Next hop: 10.1.1.2 via ge-2/0/1.0, selected
Session Id: 0x144
Next hop: 10.2.1.2 via ge-2/0/2.0, selected
Session Id: 0x145
Protocol next hop: 10.1.1.1
Indirect next hop: 0xb2b20f0 1048574 INH Session ID: 0x143
State: <Active Int Ext>
Age: 2:53 Metric2: 0
Validation State: unverified
Task: RT
Announcement bits (2): 0-KRT 2-Resolve tree 1
AS path: I
Indirect next hops: 1
  Protocol next hop: 10.1.1.1
  Indirect next hop: 0xb2b20f0 1048574 INH Session ID: 0x143
Indirect path forwarding next hops: 2
  Next hop type: Router
  Next hop: 10.1.1.2 via ge-2/0/1.0
  Session Id: 0x144
  Next hop: 10.2.1.2 via ge-2/0/2.0
  Session Id: 0x145
10.1.1.1/32 Originating RIB: inet.0
Node path count: 1
Node flags: 1
Forwarding nexthops: 2 (Merged)
Nexthop: 10.1.1.2 via ge-2/0/1.0
Nexthop: 10.2.1.2 via ge-2/0/2.0

user@host> show route active-path extensive
user@host> show route 198.51.100.1 active-path extensive
inet.0: 1000061 destinations, 1000082 routes (1000061 active, 0 holddown, 0 hidden)
198.51.100.1/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 198.51.100.1/32 -> {indirect(1051215)}
unicast reverse-path: 0
[ae0.0 ae1.0]
Page 0 idx 0, (group Internet-IPv4 type External) Type 1 val 0xbb2e53d8 (adv_entry)
Advertised metrics:
Nexthop: Self
AS path: [500] 410 I
Communities:
Path 198.51.100.1 from 10.0.0.11 Vector len 4. Val: 0
*BGP Preference: 170/-101
Next hop type: Indirect, Next hop index: 0
Address: 0xe9aad2
Next-hop reference count: 500000
Source: 10.0.0.11
Next hop type: Router, Next hop index: 0
Next hop: 10.0.0.12 via ae0.0 weight 0x1
Label operation: Push 3851, Push 25, Push 20(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 25: None; Label 20: None;
Label element ptr: 0xb5dc1780
Label parent element ptr: 0x18d48080
Label element references: 2
Label element child references: 0
Chapter 25: Protocol-Independent Routing Operational Commands

Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Label operation: Push 3851, Push 25, Push 22(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 25: None; Label 22: None;
Label element ptr: 0xb5dc1700
Label parent element ptr: 0x18d41000
Label element references: 2
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Label operation: Push 3851, Push 24, Push 48(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 24: None; Label 48: None;
Label element ptr: 0x18d40800
Label parent element ptr: 0x18d49780
Label element references: 3
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Label operation: Push 3851, Push 24, Push 49(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 24: None; Label 49: None;
Label element ptr: 0xb5dc1680
Label parent element ptr: 0x18d48f00
Label element references: 2
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Label operation: Push 3851, Push 25, Push 21(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 25: None; Label 21: None;
Label element ptr: 0xb5dc1600
Label parent element ptr: 0x18d44d80
Label element references: 2
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Label operation: Push 3851, Push 25, Push 25(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 25: None; Label 25: None;
Label element ptr: 0xb5dc1580
Label parent element ptr: 0x18d3da80
Label element references: 2
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1, selected
Label operation: Push 3851, Push 24, Push 68(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 24: None; Label 68: None;
Label element ptr: 0x18d41500
Label parent element ptr: 0x18d49000
Label element references: 3
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Label operation: Push 3851, Push 24, Push 69(top)
Label TTL action: prop-ttl, prop-ttl, prop-ttl(top)
Load balance label: Label 3851: None; Label 24: None; Label 69: None;
Label element ptr: 0xb5dc1500
Label parent element ptr: 0x18d48300
Label element references: 2
Label element child references: 0
Label element lsp id: 0
Session Id: 0x0
Protocol next hop: 10.0.0.11
Label operation: Push 3851
Label TTL action: prop-ttl
Load balance label: Label 3851: None;
Indirect next hop: 0x1883e200 1051215 INH Session ID: 0xb0d
State:
Local AS: 500 Peer AS: 500
Age: 1:40:03 Metric2: 2
Validation State: unverified
Task: BGP_500.10.0.0.11
Announcement bits (5): 0-KRT 8-KRT 9-BGP_RT_Background 10-Resolve tree 5 11-Resolve tree 8
AS path: 410 I
Accepted
Route Label: 3851
Localpref: 100
Router ID: 10.0.0.11
Indirect next hops: 1
Protocol next hop: 10.0.0.11 Metric: 2
Label operation: Push 3851
Label TTL action: prop-ttl
Load balance label: Label 3851: None;
Indirect next hop: 0x1883e200 1051215 INH Session ID: 0xb0d
Indirect path forwarding next hops (Merged): 0
Next hop type: Router
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.12.2 via ae0.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Session Id: 0x0
Next hop: 10.0.13.3 via ae1.0 weight 0x1
Session Id: 0x0
10.0.0.11/32 Originating RIB: inet.3
Metric: 1 Node path count: 4
Node flags: 1
Indirect nexthops: 4
Protocol Nexthop: 10.0.0.4 Metric: 1 Push 24
Indirect nexthop: 0x1880f200 1048597 INH Session ID: 0xb0c
Path forwarding nexthops link: 0x36120400
Path inh link: 0x0
Indirect path forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
10.0.0.4/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
Protocol Nexthop: 10.0.0.5 Metric: 1 Push 24
Indirect nexthop: 0x18810000 1048596 INH Session ID: 0xb0b
Path forwarding nexthops link: 0x1545be00
Path inh link: 0x0
Indirect path forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
10.0.0.5/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
Protocol Nexthop: 10.0.0.6 Metric: 1 Push 25
Indirect nexthop: 0x1880e600 1048588 INH Session ID: 0xb0a
Path forwarding nexthops link: 0x3611f440
Path inh link: 0x0
Indirect path forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
10.0.0.6/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
Protocol Nexthop: 10.0.0.7 Metric: 1 Push 25
Indirect nexthop: 0x1880dc00 1048586 INH Session ID: 0xb09
Path forwarding nexthops link: 0x15466d80
Path inh link: 0x0
Indirect path forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
Nexthop: 10.0.13.3 via ae1.0
Session Id: 0
10.0.0.7/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Nexthop: 10.0.12.2 via ae0.0
Session Id: 0
show route (Enhanced Subscriber Management)

```
inet.0: 41 destinations, 41 routes (40 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
198.51.100.11/24  *[Access-internal/12] 00:00:08  
> to #0 10.0.0.1.93.65 via demux0.1073741824
198.51.100.12/24  *[Access-internal/12] 00:00:08
  Private unicast
```

show route (IPv6 Flow Specification)

```
inet6.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
2001:db8::10:255:185:19/128
  *[Direct/0] 05:11:27
  > via lo0.0
2001:db8::11:11:11:0/120
  *[BGP/170] 00:28:58, localpref 100
  AS path: 2000 I, validation-state: unverified
  > to 2001:db8::13:14:2:2 via ge-1/1/4.0
2001:db8::13:14:2:0/120 *[Direct/0] 00:45:07
  > via ge-1/1/4.0
2001:db8::13:14:2:1/128 *[Local/0] 00:45:18
  Local via ge-1/1/4.0
fe80::2a0:a50f:fc71:71d5/128
  *[Direct/0] 05:11:27
  > via lo0.0
fe80::5e5e:abff:feb0:933e/128
  *[Local/0] 00:45:18
  Local via ge-1/1/4.0
inet6Flow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
2001:db8::11:11:10:10/128,*,proto=6,dstport=80,srcport=65535/term:1
  *[BGP/170] 00:28:58, localpref 100, from 2001:db8::13:14:2:2
  AS path: 2000 I, validation-state: unverified
  Fictitious
2001:db8::11:11:30/128,*,icmp6-type=128,len=100,dscp=10/term:2
  *[BGP/170] 00:20:54, localpref 100, from 2001:db8::13:14:2:2
  AS path: 2000 I, validation-state: unverified
  Fictitious
```

show route display-client-data detail

```
inet.0: 59 destinations, 70 routes (59 active, 0 holddown, 0 hidden)
198.51.100.0/24 (1 entry, 1 announced)
```
show route te-ipv4-prefix-ip

tdist.0: 283 destinations, 283 routes (283 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.10.10.10/32 } ISIS-L1:0 }/1152
  *[IS-IS/15] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0101.0101.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0202.0202.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0303.0303.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0404.0404.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0505.0505.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0606.0606.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0707.0707.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  *[IS-IS/18] 00:01:01
  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
show route te-ipv4-prefix-ip extensive

user@host>show route te-ipv4-prefix-ip 10.10.10.10 extensive

dldest: 298 destinations, 298 routes (298 active, 0 holddown, 0 hidden)
  *IS-IS Preference: 15
   Level: 1
   Next hop type: Fictitious, Next hop index: 0
   Address: 0xa1a2ac4
   Next-hop reference count: 298
   Next hop:
   State: <Active NotInstall>
   Local AS: 64496
   Age: 7:58
   Validation State: unverified
   Task: IS-IS
   AS path: I
   Prefix SID: 1000, Flags: 0x40, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0101.0101.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }
/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 298
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 7:58
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0202.0202.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }
/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 298
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 7:58
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0303.0303.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }
/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
Next-hop reference count: 298
Next hop:
State: <Active NotInstall>
Local AS: 64496
Age: 7:58
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0404.0404.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
*IS-IS Preference: 18
Level: 2
Next hop type: Fictitious, Next hop index: 0
Address: Ox1a2ac4
Next-hop reference count: 298
Next hop:
State: <Active NotInstall>
Local AS: 64496
Age: 7:58
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0505.0505.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
*IS-IS Preference: 18
Level: 2
Next hop type: Fictitious, Next hop index: 0
Address: Ox1a2ac4
Next-hop reference count: 298
Next hop:
State: <Active NotInstall>
Local AS: 64496
Age: 7:58
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0606.0606.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
*IS-IS Preference: 18
Level: 2
Next hop type: Fictitious, Next hop index: 0
Address: Ox1a2ac4
Next-hop reference count: 298
Next hop:
State: <Active NotInstall>
Local AS: 64496
Age: 7:58
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0707.0707.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
show route te-ipv4-prefix-node-iso

user@host> show route te-ipv4-prefix-node-iso 0100.0a0a.0a0a.00
lsdist.0: 283 destinations, 283 routes (283 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.10.10.10/32 } ISIS-L2:0 }/1152
  * [IS-IS/18] 00:05:20  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.2.2.2/32 } ISIS-L2:0 }/1152
  * [IS-IS/18] 00:05:20  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.3.3.3/32 } ISIS-L2:0 }/1152
  * [IS-IS/18] 00:05:20  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.4.4.4/32 } ISIS-L2:0 }/1152
  * [IS-IS/18] 00:05:20  Fictitious
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.5.5.5/32 } ISIS-L2:0 }/1152
  * [IS-IS/18] 00:05:20  Fictitious

showroutete-ipv4-prefix-node-iso
show route te-ipv4-prefix-node-iso extensive

user@host> show route te-ipv4-prefix-node-iso 0100.0a0a.0a0a.00 extensive

lsdist.0: 283 destinations, 283 routes (283 active, 0 holddown, 0 hidden)
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.10.10.10/32 } ISIS-L1:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 15
  Level: 1
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS:  64496
  Age: 6:47
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1000, Flags: 0x40, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.1.1.1/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS:  64496
  Age: 6:47
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1001, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.2.2.2/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
State: <Active NotInstall>
Local AS: 64496
Age: 6:47
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1002, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.3.3.3/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: Oxala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
Local AS: 64496
Age: 6:47
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1003, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.4.4.4/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: Oxala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
Local AS: 64496
Age: 6:47
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1004, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.5.5.5/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: Oxala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
Local AS: 64496
Age: 6:47
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1005, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.6.6.6/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2

2268 Copyright © 2019, Juniper Networks, Inc.
 show route te-ipv4-prefix-node-iso detail

user@host> show route te-ipv4-prefix-node-iso 0100.0a0a.0a0a.00 detail

lsdist.0: 283 destinations, 283 routes (283 active, 0 holddown, 0 hidden)
PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.10.10.10/32 } ISIS-L1:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 15
  Level: 1
  Next hop type: Fictitious, Next hop index: 0
  Address: Oxala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 6:47
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1000, Flags: 0xe0, Algo: 0

show route te-ipv4-prefix-node-isodetail
Age: 6:54
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0x40, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.1.1.1/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 6:54
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1001, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.2.2.2/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 6:54
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1002, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.3.3.3/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xala2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS: 64496
  Age: 6:54
  Validation State: unverified
  Task: IS-IS
  AS path: I
  Prefix SID: 1003, Flags: 0xe0, Algo: 0

PREFIX { Node { AS:64496 ISO:0100.0a0a.0a0a.00 } { IPv4:10.4.4.4/32 } ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xala2ac4
Next-hop reference count: 283
Next hop:
State: <Active NotInstall>
Local AS:  64496
Age: 6:54
Validation State: unverified
Task:  IS-IS
AS path:  I
Prefix SID:  1004, Flags: 0xe0, Algo: 0

PREFIX { Node {  AS:64496 ISO:0100.0a0a.0a0a.00 }  { IPv4:10.5.5.5/32 }  ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS:  64496
  Age: 6:54
  Validation State: unverified
  Task:  IS-IS
  AS path:  I
  Prefix SID:  1005, Flags: 0xe0, Algo: 0

PREFIX { Node {  AS:64496 ISO:0100.0a0a.0a0a.00 }  { IPv4:10.6.6.6/32 }  ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS:  64496
  Age: 6:54
  Validation State: unverified
  Task:  IS-IS
  AS path:  I
  Prefix SID:  1006, Flags: 0xe0, Algo: 0

PREFIX { Node {  AS:64496 ISO:0100.0a0a.0a0a.00 }  { IPv4:10.7.7.7/32 }  ISIS-L2:0 }/1152 (1 entry, 0 announced)
  *IS-IS  Preference: 18
  Level: 2
  Next hop type: Fictitious, Next hop index: 0
  Address: 0xa1a2ac4
  Next-hop reference count: 283
  Next hop:
  State: <Active NotInstall>
  Local AS:  64496
  Age: 6:54
  Validation State: unverified
  Task:  IS-IS
  AS path:  I
  Prefix SID:  1007, Flags: 0xe0, Algo: 0

PREFIX { Node {  AS:64496 ISO:0100.0a0a.0a0a.00 }  { IPv4:10.10.10.10/32 }  ISIS-L2:0 }/1152 (1 entry, 0 announced)
*IS-IS  Preference: 18
Level: 2
Next hop type: Fictitious, Next hop index: 0
Address: 0xa1a2ac4
Next-hop reference count: 283
Next hop:
State: <Active NotInstall>
Local AS:   64496
Age: 6:54
Validation State: unverified
Task: IS-IS
AS path: I
Prefix SID: 1000, Flags: 0x40, Algo: 0
show route active-path

List of Syntax  Syntax on page 2273
Syntax (EX Series Switches) on page 2273

Syntax  
show route active-path
   <brief | detail | extensive | terse>
   <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  
show route active-path
   <brief | detail | extensive | terse>

Release Information  
Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Display all active routes for destinations. An active route is a route that is selected as the best path. Inactive routes are not displayed.

Options  
none—Display all active routes.

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.

Required Privilege  
view

List of Sample Output  
show route active-path on page 2273
show route active-path brief on page 2274
show route active-path detail on page 2274
show route active-path extensive on page 2275
show route active-path terse on page 2277

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 active-path

user@host> show route active-path
inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
show route active-path brief

The output for the `show route active-path brief` command is identical to that for the `show route active-path` command. For sample output, see `show route active-path` on page 2273.

show route active-path detail

```
user@host> show route active-path detail

inet0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)

10.255.70.19/32 (1 entry, 1 announced)
  ^[Direct/0] 21:33:52
    > via lo0.0

10.255.71.50/32  ^[IS-IS/15] 00:18:13, metric 10
    > to 172.16.100.1 via so-2/1/3.0

172.16.100.1/24  ^[Direct/0] 00:18:36
    > via so-2/1/3.0

172.16.100.1/32  ^[Local/0] 00:18:41
    Local via so-2/1/3.0

192.168.64.0/21  ^[Direct/0] 21:33:52
    > via fxp0.0

192.168.70.19/32  ^[Local/0] 21:33:52
    Local via fxp0.0
```
show route active-path extensive

inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
10.255.70.19/32 (1 entry, 1 announced)
TSI:
IS-IS level 1, LSP fragment 0
IS-IS level 2, LSP fragment 0
  ^Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 3
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS: 200
  Age: 21:37:10
  Task: IF
  Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

172.16.100.1/32 (1 entry, 1 announced)
  ^Local Preference: 0
  Next hop type: Local
  Next-hop reference count: 11
  Interface: so-2/1/3.0
  State: <Active NoReadvrt Int>
  Local AS: 200
  Age: 21:59
  Task: IF
  Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

192.168.64.0/21 (1 entry, 1 announced)
  ^Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 3
  Next hop: via fxp0.0, selected
  State: <Active Int>
  Local AS: 200
  Age: 21:37:10
  Task: IF
  Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

192.168.70.19/32 (1 entry, 1 announced)
  ^Local Preference: 0
  Next hop type: Local
  Next-hop reference count: 11
  Interface: fxp0.0
  State: <Active NoReadvrt Int>
  Local AS: 200
  Age: 21:37:10
  Task: IF
  Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
  AS path: I
Age: 21:39:47  
Task: IF  
Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3  
AS path: I  

10.255.71.50/32 (1 entry, 1 announced)  
TSI:  
KRT in-kernel 10.255.71.50/32 --> {172.16.100.1}  
IS-IS level 2, LSP fragment 0  
  *IS-IS Preference: 15  
    Level: 1  
    Next hop type: Router, Next hop index: 397  
    Next-hop reference count: 4  
    Next hop: 172.16.100.1 via so-2/1/3.0, selected  
    State: <Active Int>  
    Local AS:  200  
    Age: 24:08  
    Metric: 10  
    Task: IS-IS  
    Announcement bits (4): 0-KRT 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3  
    AS path: I  

172.16.100.1/24 (1 entry, 1 announced)  
TSI:  
IS-IS level 1, LSP fragment 0  
IS-IS level 2, LSP fragment 0  
  *Direct Preference: 0  
    Next hop type: Interface  
    Next-hop reference count: 3  
    Next hop: via so-2/1/3.0, selected  
    State: <Active Int>  
    Local AS:  200  
    Age: 24:31  
    Task: IF  
    Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3  
    AS path: I  

172.16.100.1/32 (1 entry, 1 announced)  
  *Local Preference: 0  
    Next hop type: Local  
    Next-hop reference count: 11  
    Interface: so-2/1/3.0  
    State: <Active NoReadvrt Int>  
    Local AS:  200  
    Age: 24:36  
    Task: IF  
    Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3  
    AS path: I  

192.168.64.0/21 (1 entry, 1 announced)  
  *Direct Preference: 0  
    Next hop type: Interface  
    Next-hop reference count: 3  
    Next hop: via fxp0.0, selected  
    State: <Active Int>  
    Local AS:  200  
    Age: 21:39:47  
    Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I
192.168.70.19/32 (1 entry, 1 announced)
  *Local  Preference: 0
   Next-hop type: Local
   Next-hop reference count: 11
   Interface: fxp0.0
   State: <Active NoReadvrt Int>
   Local AS: 200
   Age: 21:39:47
   Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

show route active-path terse

user@host> show route active-path terse
 inert.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
 + = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.255.70.19/32</td>
<td>D 0</td>
<td>0</td>
<td>&gt;lo0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.50/32</td>
<td>I 15</td>
<td>10</td>
<td>&gt;172.16.100.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 172.16.100.0/24</td>
<td>D 0</td>
<td>0</td>
<td>&gt;so-2/1/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 172.16.100.2/32</td>
<td>L 0</td>
<td></td>
<td>Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 192.168.64.0/21</td>
<td>D 0</td>
<td></td>
<td>&gt;fxp0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 192.168.70.19/32</td>
<td>L 0</td>
<td></td>
<td>Local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show route advertising-protocol

Syntax

show route advertising-protocol protocol neighbor-address
   <brief | detail | extensive | terse>
   <logical-system (all | logical-system-name)>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display the routing information as it has been prepared for advertisement to a particular neighbor of a particular dynamic routing protocol.

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor-address—Address of the neighboring router to which the route entry is being transmitted.

protocol—Protocol transmitting the route:

- bgp—Border Gateway Protocol
- dvmrp—Distance Vector Multicast Routing Protocol
- msdp—Multicast Source Discovery Protocol
- pim—Protocol Independent Multicast
- rip—Routing Information Protocol
- ripng—Routing Information Protocol next generation

Additional Information

Routes displayed are routes that the routing table has exported into the routing protocol and that have been filtered by the associated protocol's export routing policy statements. Starting with Junos OS Release 13.3, you can display the routing instance table foo for any address family, on a VPN route reflector, or a VPN AS boundary router that is advertising local VPN routes. However, if you do not specify the table in the command, the output displays each VRF prefix twice.

Required Privilege

view

Related Documentation

- Example: Configuring the MED Attribute That Determines the Exit Point in an AS

List of Sample Output

show route advertising-protocol bgp (Layer 3 VPN) on page 2281
show route advertising-protocol bgp detail on page 2281
show route advertising-protocol bgp detail (Aggregate Extended Community Bandwidth) on page 2281
show route advertising-protocol bgp detail (Labeled Unicast) on page 2282
show route advertising-protocol bgp detail (Layer 2 VPN) on page 2282
show route advertising-protocol bgp detail (Layer 3 VPN) on page 2282
show route advertising-protocol bgp extensive all (Next Hop Self with RIB-out IP Address) on page 2283

Output Fields  Table 169 on page 2279 lists the output fields for the show route advertising-protocol command. Output fields are listed in the approximate order in which they appear.

Table 169: show route advertising-protocol Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table—for example, inet.0.</td>
<td>All levels</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
<td>All levels</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)  
  • hold down (routes that are in the pending state before being declared inactive)  
  • hidden (routes that are not used because of a routing policy) | All levels      |
| Prefix                  | Destination prefix.                                                              | brief none      |
| destination-prefix      | Destination prefix. The entry value is the number of routes for this destination, and the announced value is the number of routes being announced for this destination. | detail extensive |
| BGP group and type      | BGP group name and type (Internal or External).                                   | detail extensive |
| Route Distinguisher     | Unique 64-bit prefix augmenting each IP subnet.                                   | detail extensive |
| Advertised Label        | Incoming label advertised by the Label Distribution Protocol (LDP). When an IP packet enters a label-switched path (LSP), the ingress router examines the packet and assigns it a label based on its destination, placing the label in the packet's header. The label transforms the packet from one that is forwarded based on its IP routing information to one that is forwarded based on information associated with the label. | detail extensive |
| Label-Base, range       | First label in a block of labels and label block size. A remote PE router uses this first label when sending traffic toward the advertising PE router. | detail extensive |
| VPN Label               | Virtual private network (VPN) label. Packets are sent between CE and PE routers by advertising VPN labels. VPN labels transit over either a Resource Reservation Protocol (RSVP) or a Label Distribution Protocol (LDP) label-switched path (LSP) tunnel. | detail extensive |
### Table 169: show route advertising-protocol 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>Nexthop</strong></td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route. If the next-hop advertisement to the peer is <strong>Self</strong>, and the RIB-out next hop is a specific IP address, the RIB-out IP address is included in the extensive output. See show route advertising-protocol bgp extensive all (Next Hop Self with RIB-out IP Address) on page 2283.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MED</strong></td>
<td>Multiple exit discriminator value included in the route.</td>
<td><strong>brief</strong></td>
</tr>
<tr>
<td><strong>Lclpref or Localpref</strong></td>
<td>Local preference value included in the route.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Queued</strong></td>
<td>When BGP route prioritization is enabled and a route is present in a priority queue, this shows which priority queue the route is in.</td>
<td>All levels except <strong>brief</strong></td>
</tr>
</tbody>
</table>
| **AS path** | 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:  
  - I—IGP.  
  - E—EGP.  
  - ?—Incomplete; typically, the AS path was aggregated.  
  When AS path numbers are included in the route, the format is as follows:  
  - [ ]—Brackets enclose the local AS number associated with the AS path if configured on the router, or if AS path prepending is configured.  
  - { }—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.  
  - ( )—Parentheses enclose a confederation.  
  - ( [ ])—Parentheses and brackets enclose a confederation set.  
  **NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance. | All levels |
| **Route Labels** | Stack of labels carried in the BGP route update. | **detail extensive** |
| **Cluster list** | (For route reflected output only) Cluster ID sent by the route reflector. | **detail extensive** |
| **Originator ID** | (For route reflected output only) Address of routing device that originally sent the route to the route reflector. | **detail extensive** |
| **Communities** | Community path attribute for the route. See the output field table for the show route detail command for all possible values for this field. | **detail extensive** |
| **AIGP** | Accumulated interior gateway protocol (AIGP) BGP attribute. | **detail extensive** |
Table 169: show route advertising-protocol Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attrset AS</td>
<td>Number, local preference, and path of the autonomous system (AS) that originated the route. These values are stored in the Attrset attribute at the originating router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Layer2-info:encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show route advertising-protocol bgp (Layer 3 VPN)

```plaintext
user@host> show route advertising-protocol bgp 10.255.14.171

VPN-A.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix            Nexthop                MED    Lclpref AS path
10.255.14.172/32  Self                     1        100 I

VPN-B.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix            Nexthop                MED    Lclpref AS path
10.255.14.181/32  Self                     2        100 I
```

show route advertising-protocol bgp detail

```plaintext
user@host> show route advertising-protocol bgp 111.222.1.3 detail

bgp20.inet.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
111.222.1.11/32 (1 entry, 1 announced)
BGP group pe-pe type Internal
  Route Distinguisher: 111.255.14.11:69
  Advertised Label: 100000
  next hop: Self
  Localpref: 100
  AS path: 2 I
  Communities: target:69:20
  AIGP 210
111.8.0.0/16 (1 entry, 1 announced)
BGP group pe-pe type Internal
  Route Distinguisher: 111.255.14.11:69
  Advertised Label: 100000
  next hop: Self
  Localpref: 100
  AS path: 2 I
  Communities: target:69:20
  AIGP 210
```

show route advertising-protocol bgp detail (Aggregate Extended Community Bandwidth)

```plaintext
user@host> show route advertising-protocol bgp 10.0.4.2 10.0.2.0/30 detail

inet.0: 20 destinations, 26 routes (20 active, 0 holddown, 0 hidden)
  * 10.0.2.0/30 (2 entries, 1 announced)
```
BGP group external2 type External
Nexthop: Self
AS path: [65000] 65001 I
Communities: bandwidth:65000:80000000

show route advertising-protocol bgp detail (Labeled Unicast)

user@host> show route advertising bgp 1.1.1.3 detail

inet.0: 69 destinations, 70 routes (69 active, 0 holddown, 0 hidden)
* 1.1.1.8/32 (2 entries, 2 announced)
BGP group ibgp type Internal
Route Labels: 1000123(top) 1000124 1000125 1000126
Nexthop: 1.1.1.4
MED: 7
Localpref: 100
AS path: [5] I
Cluster ID: 3.3.3.3
Originator ID: 1.1.1.1
Entropy label capable

inet6.0: 26 destinations, 28 routes (26 active, 0 holddown, 0 hidden)
* 100::1/128 (2 entries, 1 announced)
BGP group ibgp type Internal
Labels: 1000123(top) 1000124 1000125 1000126
Nexthop: ::ffff:1.1.1.4
Localpref: 100
AS path: [5] I
Cluster ID: 3.3.3.3
Originator ID: 1.1.1.1

show route advertising-protocol bgp detail (Layer 2 VPN)

user@host> show route advertising-protocol bgp 192.168.24.1 detail

vpn-a.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
192.168.16.1:1:1:1/96 (1 entry, 1 announced)
BGP group int type Internal
Route Distinguisher: 192.168.16.1:1
Label-base : 32768, range : 3
Nexthop: Self
Localpref: 100
AS path: I
Communities: target:65412:100
AIGP 210
Layer2-info: encaps:VLAN, control flags:, mtu:

show route advertising-protocol bgp detail (Layer 3 VPN)

user@host> show route advertising-protocol bgp 10.255.14.176 detail

vpna.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
* 10.49.0.0/30 (1 entry, 1 announced)
BGP group ibgp type Internal
Route Distinguisher: 10.255.14.174:2
VPN Label: 101264
Nexthop: Self
Localpref: 100
AS path: I
Communities: target:200:100

Copyright © 2019, Juniper Networks, Inc.
show route advertising-protocol bgp extensive all (Next Hop Self with RIB-out IP Address)

user@host> show route advertising-protocol bgp 200.0.1.0/24 extensive all

inet.0: 13 destinations, 19 routes (13 active, 0 holddown, 6 hidden)
170.0.1.0/24 (2 entries, 1 announced)
  BGP group eBGP-INTEROP type External
  Nexthop: Self (rib-out 10.100.3.2)
  AS path: [4713] 200 I

...
### show route all

**List of Syntax**
- Syntax on page 2284
- Syntax (EX Series Switches) on page 2284

**Syntax**
```
  show route all
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
- show route all

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display information about all routes in all routing tables, including private, or internal, tables.

**Options**
- `none`—Display information about all routes in all routing tables, including private, or internal, tables.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
- view

**Related Documentation**
- show route brief on page 2291
- show route detail on page 2304

**List of Sample Output**
- show route all on page 2284

**Output Fields**
In Junos OS Release 9.5 and later, only the output fields for the `show route all` command display all routing tables, including private, or hidden, routing tables. The output field table of the `show route` command does not display entries for private, or hidden, routing tables in Junos OS Release 9.5 and later.

**Sample Output**
```
show route all
```

The following example displays a snippet of output from the `show route` command and then displays the same snippet of output from the `show route all` command:
```
user@host> show route
```
mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
0                  *[MPLS/0] 2d 02:24:39, metric 1
  Receive
1                  *[MPLS/0] 2d 02:24:39, metric 1
  Receive
2                  *[MPLS/0] 2d 02:24:39, metric 1
  Receive
800017             *[VPLS/7] 1d 14:00:16
  > via vt-3/2/0.32769, Pop
800018             *[VPLS/7] 1d 14:00:26
  > via vt-3/2/0.32772, Pop

user@host> show route all

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
0                  *[MPLS/0] 2d 02:19:12, metric 1
  Receive
1                  *[MPLS/0] 2d 02:19:12, metric 1
  Receive
2                  *[MPLS/0] 2d 02:19:12, metric 1
  Receive
800017             *[VPLS/7] 1d 13:54:49
  > via vt-3/2/0.32769, Pop
800018             *[VPLS/7] 1d 13:54:59
  > via vt-3/2/0.32772, Pop
vt-3/2/0.32769     [VPLS/7] 1d 13:54:49
  Unusable
vt-3/2/0.32772     [VPLS/7] 1d 13:54:59
  Unusable
**show route aspath-regex**

**List of Syntax**  
Syntax on page 2286  
Syntax (EX Series Switches) on page 2286

**Syntax**  
`show route aspath-regex regular-expression`  
`<logical-system (all | logical-system-name)>`

**Syntax (EX Series Switches)**  
`show route aspath-regex regular-expression`

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

**Description**  
Display the entries in the routing table that match the specified autonomous system (AS) path regular expression.

**Options**  
`regular-expression`—Regular expression that matches an entire AS path.  
`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**  
You can specify a regular expression as:

- An individual AS number
- A period wildcard used in place of an AS number
- An AS path regular expression that is enclosed in parentheses

You also can include the operators described in the table of AS path regular expression operators in the *Junos Policy Framework Configuration Guide*. The following list summarizes these operators:

- `{m,n}`—At least `m` and at most `n` repetitions of the AS path term.
- `{m}`—Exactly `m` repetitions of the AS path term.
- `{m,}`—`m` or more repetitions of the AS path term.
- `*`—Zero or more repetitions of an AS path term.
- `+`—One or more repetitions of an AS path term.
- `?`—Zero or one repetition of an AS path term.
- `aspath_term | aspath_term`—Match one of the two AS path terms.

When you specify more than one AS number or path term, or when you include an operator in the regular expression, enclose the entire regular expression in quotation marks. For example, to match any path that contains AS number 234, specify the following command:
show route aspath-regex ".*234.*"

**Required Privilege**  
view

**Level**

**Related Documentation**

- Example: Using AS Path Regular Expressions

**List of Sample Output**

- show route aspath-regex (Matching a Specific AS Number) on page 2287
- show route aspath-regex (Matching Any Path with Two AS Numbers) on page 2287

**Output Fields**

For information about output fields, see the output field table for the show route command.

**Sample Output**

**show route aspath-regex (Matching a Specific AS Number)**

```
user@host> show route aspath-regex 65477
inet.0: 46411 destinations, 46411 routes (46409 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

111.222.1.0/25   *[BGP/170] 00:08:48, localpref 100, from 111.222.2.24
    AS Path: [65477] ({65548 65536}) IGP
to 111.222.18.225 via fpa0.0(111.222.18.233)
111.222.1.128/25  *[15-15/15] 09:15:37, metric 37, tag 1
to 111.222.18.225 via fpa0.0(111.222.18.233)
    [BGP/170] 00:08:48, localpref 100, from 111.222.2.24
    AS Path: [65477] ({65548 65536}) IGP
to 111.222.18.225 via fpa0.0(111.222.18.233)
...```

**show route aspath-regex (Matching Any Path with Two AS Numbers)**

```
user@host> show route aspath-regex ".*234 3561.*"
inet.0: 46351 destinations, 46351 routes (46349 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

9.20.0.0/17     *[BGP/170] 01:35:00, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 2685 2686 Incomplete
to 192.156.169.1 via 192.156.169.14(so-0/0/0)
12.10.231.0/24  *[BGP/170] 01:35:00, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 5696 7369 IGP
to 192.156.169.1 via 192.156.169.14(so-0/0/0)
24.64.32.0/19   *[BGP/170] 01:34:59, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 6327 IGP
to 192.156.169.1 via 192.156.169.14(so-0/0/0)
...```
show route best

List of Syntax

Syntax on page 2288
Syntax (EX Series Switches) on page 2288

Syntax

show route best destination-prefix
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route best destination-prefix
  <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.

Description

Display the route in the routing table that is the best route to the specified address or range of addresses. The best route is the longest matching route.

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.

destination-prefix—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

Related Documentation

• show route brief on page 2291
• show route detail on page 2304

List of Sample Output

show route best on page 2289
show route best detail on page 2289
show route best extensive on page 2290
show route best terse on page 2290

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 best

user@host> show route best 10.255.70.103

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.255.70.103/32  *[OSPF/10] 1d 13:19:20, metric 2
  > to 10.31.1.6 via ge-3/1/0.0
    via so-0/3/0.0

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.255.70.103/32  *[RSVP/7] 1d 13:20:13, metric 2
  > via so-0/3/0.0, label-switched-path green-r1-r3

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.0.0.0/8        *[Direct/0] 2d 01:43:34
  > via fxp2.0
  > via fxp1.0

show route best detail

user@host> show route best 10.255.70.103 detail

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
10.255.70.103/32 (1 entry, 1 announced)
  *OSPF  Preference: 10
  Next-hop reference count: 9
  Next hop: 10.31.1.6 via ge-3/1/0.0, selected
  Next hop: via so-0/3/0.0
  State: <Active Int>
  Local AS:    69
  Age: 1d 13:20:06        Metric: 2
  Area: 0.0.0.0
  Task: OSPF
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
10.255.70.103/32 (1 entry, 1 announced)
  *RSVP  Preference: 7
  Next-hop reference count: 5
  Next hop: via so-0/3/0.0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 100016
  State: <Active Int>
  Local AS:    69
  Age: 1d 13:20:59        Metric: 2
  Task: RSVP
  Announcement bits (1): 1-Resolve tree 2
  AS path: I
### show route best extensive

The output for the `show route best extensive` command is identical to that for the `show route best detail` command. For sample output, see `show route best detail` on page 2289.

### show route best terse

```bash
user@host> show route best 10.255.70.103 terse
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.255.70.103/32</td>
<td>O 10</td>
<td>2</td>
<td>&gt;10.31.1.6</td>
<td>so-0/3/0.0</td>
<td></td>
</tr>
</tbody>
</table>

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.255.70.103/32</td>
<td>R 7</td>
<td>2</td>
<td>&gt;so-0/3/0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.0.0.0/8</td>
<td>D 0</td>
<td></td>
<td>&gt;fp2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D 0</td>
<td></td>
<td></td>
<td>&gt;fp1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show route brief

List of Syntax  Syntax on page 2291
               Syntax (EX Series Switches) on page 2291

Syntax  show route brief
       <destination-prefix>
       <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route brief
                                <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 brief 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  view

Level

Related Documentation  • show route all on page 2284
                      • show route best on page 2288

List of Sample Output  show route brief on page 2291

Output Fields  For information about output fields, see the Output Field table of the show route command.

Sample Output

show route brief
user@host> show route brief
inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0       *[Static/5] 1w5d 20:30:29
<table>
<thead>
<tr>
<th>Address</th>
<th>Type</th>
<th>Age</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.51/32</td>
<td>Direct</td>
<td>2w4d</td>
<td>via lo0.0</td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td>Static</td>
<td>2w4d</td>
<td>to 192.168.167.254 via fxp0.0</td>
</tr>
<tr>
<td>192.168.0.0/18</td>
<td>Static</td>
<td>2w4d</td>
<td>to 192.168.167.254 via fxp0.0</td>
</tr>
<tr>
<td>192.168.40.0/22</td>
<td>Static</td>
<td>2w4d</td>
<td>to 192.168.167.254 via fxp0.0</td>
</tr>
<tr>
<td>192.168.64.0/18</td>
<td>Static</td>
<td>2w4d</td>
<td>to 192.168.167.254 via fxp0.0</td>
</tr>
<tr>
<td>192.168.164.0/22</td>
<td>Direct</td>
<td>2w4d</td>
<td>via fxp0.0</td>
</tr>
<tr>
<td>192.168.164.51/32</td>
<td>Local</td>
<td>2w4d</td>
<td>Local via fxp0.0</td>
</tr>
<tr>
<td>207.17.136.192/32</td>
<td>Static</td>
<td>2w4d</td>
<td>to 192.168.167.254 via fxp0.0</td>
</tr>
<tr>
<td>green.inet.0:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.101.0.0/16</td>
<td>Direct</td>
<td>1w5d</td>
<td>via fe-0/0/3.0</td>
</tr>
<tr>
<td>100.101.2.3/32</td>
<td>Local</td>
<td>1w5d</td>
<td>Local via fe-0/0/3.0</td>
</tr>
<tr>
<td>172.16.233.5/32</td>
<td>OSPF</td>
<td>1w5d</td>
<td>via fe-0/0/3.0</td>
</tr>
</tbody>
</table>

Discard

Copyright © 2019, Juniper Networks, Inc.
show route ccc

Syntax

show route ccc ccc
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display circuit cross-connect (CCC) entries in the Multiprotocol Link Switching (MPLS) routing table.

Options

ccc—Name of an entry with a circuit cross-connect interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

Related Documentation

• show connections

List of Sample Output

show route ccc extensive on page 2293

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 ccc extensive

user@host> show route ccc fe-0/1/0.600 extensive

mpls.0: 19 destinations, 19 routes (19 active, 0 holddown, 0 hidden)
fe-0/1/2.600 (1 entry, 1 announced)
TSI:
KRT in-kernel fe-0/1/2.600.0 /16 -> {0.0.0.0}

Preference: 7
Next-hop reference count: 2
Next hop: via so-0/0/3.0 weight 0x1, selected
Label operation: Push 101424
State: <Active Int>
Local AS: 100
Age: 28:13 Metric: 3
Task: MPLS
Announcement bits (1): 0-KRT
AS path: I
show route community

**List of Syntax**
- Syntax on page 2295
- Syntax (EX Series Switches) on page 2295

**Syntax**
```
show route community as-number:community-value
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route community as-number:community-value
  <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.

**Description**
Display the route entries in each routing table that are members of a Border Gateway Protocol (BGP) community.

**Options**
- **as-number:community-value**—One or more community identifiers. **as-number** is the AS number, and **community-value** is the community identifier. When you specify more than one community identifier, enclose the identifiers in double quotation marks. Community identifiers can include wildcards.

  For example:

  ```
  user@host> show route table inet.0 protocol bgp community "12083:6015"
  community "12083:65551"
  
  or
  
  user@host> show route table inet.0 protocol bgp community [12083:6014 12083:65551]
  
  brief | detail | extensive | terse—(Optional) Display the specified level of output.
  logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
```

**Additional Information**
Specifying the community option displays all routes matching the community found within the routing table. The community option does not limit the output to only the routes being advertised to the neighbor after any egress routing policy.

**Required Privilege**
- view

---

Chapter 25: Protocol-Independent Routing Operational Commands
List of Sample Output

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 community

user@host> show route community 234:80
inet.0: 46511 destinations, 46511 routes (46509 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.4.0/8      *[BGP/170] 03:33:07, localpref 100, from 131.103.20.49
                  AS Path: (666) 234 2548 1 IGP
                  to 192.156.169.1 via 192.156.169.14(so-0/0/0)
172.16.6.0/8      *[BGP/170] 03:33:07, localpref 100, from 131.103.20.49
                  AS Path: (666) 234 2548 568 721 Incomplete
                  to 192.156.169.1 via 192.156.169.14(so-0/0/0)
172.16.92.0/16    *[BGP/170] 03:33:06, localpref 100, from 131.103.20.49
                  AS Path: (666) 234 2548 1673 1675 1747 IGP
                  to 192.156.169.1 via 192.156.169.14(so-0/0/0)
**show route community-name**

**List of Syntax**

Syntax on page 2297  
Syntax (EX Series Switches) on page 2297

**Syntax**

show route community-name community-name  
<brief | detail | extensive | terse>  
<logical-system (all | logical-system-name)>  

**Syntax (EX Series Switches)**

show route community-name community-name  
<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.

**Description**

Display the route entries in each routing table that are members of a Border Gateway Protocol (BGP) community, specified by a community name.

**Options**

*community-name*—Name of the community.  
*brief | detail | extensive | terse*—(Optional) Display the specified level of output.  
*logical-system (all | logical-system-name)*—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

view

**List of Sample Output**

show route community-name on page 2297

**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 community-name

```
user@host> show route community-name red-com
inet.0: 17 destinations, 17 routes (16 active, 0 holddown, 1 hidden)
inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
instance1.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
red.inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```
<table>
<thead>
<tr>
<th>IP Address</th>
<th>BGP Details</th>
<th>AS Path</th>
<th>NextHop</th>
<th>Label-Switched Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.212/32</td>
<td>*[BGP/170] 00:04:40, localpref 100, from 10.255.245.204</td>
<td>300 I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
<tr>
<td>172.16.20.20/32</td>
<td>*[BGP/170] 00:04:40, localpref 100, from 10.255.245.204</td>
<td>I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
<tr>
<td>172.16.100.0/24</td>
<td>*[BGP/170] 00:04:40, localpref 100, from 10.255.245.204</td>
<td>I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
</tbody>
</table>

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
bgp.l3vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>IP Address</th>
<th>BGP Details</th>
<th>AS Path</th>
<th>NextHop</th>
<th>Label-Switched Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.204:10:10.255.245.212/32</td>
<td>*[BGP/170] 00:06:40, localpref 100, from 10.255.245.204</td>
<td>300 I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
<tr>
<td>10.255.245.204:10:172.16.20.20/32</td>
<td>*[BGP/170] 00:36:02, localpref 100, from 10.255.245.204</td>
<td>I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
<tr>
<td>10.255.245.204:10:100.1.4.0/24</td>
<td>*[BGP/170] 00:36:02, localpref 100, from 10.255.245.204</td>
<td>I</td>
<td>to 172.16.100.1 via ge-1/1/0.0, label-switched-path to <em>fix</em></td>
<td></td>
</tr>
</tbody>
</table>

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
instance1.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
**show route damping**

**List of Syntax**

Syntax (EX Series Switch and QFX Series) on page 2299

Syntax

show route damping (decayed | history | suppressed)

<brief | detail | extensive | terse>

<logical-system (all | logical-system-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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display the BGP routes for which updates might have been reduced because of route flap damping.

**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.

decayed—Display route damping entries that might no longer be valid, but are not suppressed.

history—Display entries that have already been withdrawn, but have been logged.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

suppressed—Display entries that have been suppressed and are no longer being installed into the forwarding table or exported by routing protocols.

**Required Privilege**

view

**Related Documentation**

• clear bgp damping on page 1730

• show policy damping on page 1777

**List of Sample Output**

show route damping decayed detail on page 2302

show route damping history on page 2303

show route damping history detail on page 2303
Output Fields  Table 170 on page 2300 lists the output fields for the `show route damping` command. Output fields are listed in the approximate order in which they appear.

Table 170: `show route damping` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table—for example, <code>inet.0</code>.</td>
<td>All levels</td>
</tr>
<tr>
<td>destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• active</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• holddown (routes that are in a pending state before being declared inactive)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hidden (the routes are not used because of a routing policy)</td>
<td></td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Destination prefix. The <code>entry</code> value is the number of routes for this destination, and the <code>announced</code> value is the number of routes being announced for this destination.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[protocol, preference]</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• -—A hyphen indicates the last active route.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• *—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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In every routing metric except for the BGP <code>LocalPref</code> attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the <code>LocalPref</code> value in the <code>Preference2</code> field. For example, if the <code>LocalPref</code> value for Route 1 is 100, the <code>Preference2</code> value is -101. If the <code>LocalPref</code> value for Route 2 is 155, the <code>Preference2</code> value is -156. Route 2 is preferred because it has a higher <code>LocalPref</code> value and a lower <code>Preference2</code> value.</td>
<td></td>
</tr>
<tr>
<td>Next-hop reference count</td>
<td>Number of references made to the next hop.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Source</td>
<td>IP address of the route source.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Next hop</td>
<td>Network layer address of the directly reachable neighboring system.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>via</td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word <code>Selected</code>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol next hop</td>
<td>Network layer address of the remote routing device that advertised the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>This address is used to derive a forwarding next hop.</td>
<td></td>
</tr>
<tr>
<td>Indirect next hop</td>
<td>Index designation used to specify the mapping between protocol next hops, tags, kernel export policy, and the forwarding next hops.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 170: `show route damping` 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>Flags for this route. For a description of possible values for this field, see the output field table for the <code>show route detail</code> command.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local AS</td>
<td>AS number of the local routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Peer AS</td>
<td>AS number of the peer routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Age</td>
<td>How long the route has been known.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric for the route.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>List of protocols that announce this route. <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>
<td>detail extensive</td>
</tr>
<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>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When AS path numbers are included in the route, the format is as follows:</td>
<td></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>
<td></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>
<td></td>
</tr>
<tr>
<td></td>
<td>• ( )—Parentheses enclose a confederation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ( [ ] )—Parentheses and brackets enclose a confederation set.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</td>
<td></td>
</tr>
<tr>
<td>to</td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route.</td>
<td>brief none</td>
</tr>
<tr>
<td>via</td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word <code>Selected</code>.</td>
<td>brief none</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See the output field table for the <code>show route detail</code> command.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 170: show route damping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localpref</td>
<td>Local preference value included in the route.</td>
<td>All levels</td>
</tr>
<tr>
<td>Router ID</td>
<td>BGP router ID as advertised by the neighbor in the open message.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Merit (last update/nw)</td>
<td>Last updated and current figure-of-merit value.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>damping-parameters</td>
<td>Name that identifies the damping parameters used, which is defined in the damping statement at the [edit policy-options] hierarchy level.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last update</td>
<td>Time of most recent change in path attributes.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>First update</td>
<td>Time of first change in path attributes, which started the route damping process.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the route has gone up or down or its path attributes have changed.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Suppressed</td>
<td>(suppressed keyword only) This route is currently suppressed. A suppressed route does not appear in the forwarding table and routing protocols do not export it.</td>
<td>All levels</td>
</tr>
<tr>
<td>Reusable in</td>
<td>(suppressed keyword only) Time when a suppressed route will again be available.</td>
<td>All levels</td>
</tr>
<tr>
<td>Preference will be</td>
<td>(suppressed keyword only) Preference value that will be applied to the route when it is again active.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show route damping decayed detail

user@host> show route damping decayed detail
inet.0: 173319 destinations, 1533668 routes (172625 active, 4 holddown, 108083 hidden)
10.0.111.0/24 (7 entries, 1 announced)
*BGP
  Preference: 170/-101
  Next-hop reference count: 151973
  Source: 172.23.2.129
  Next hop: via so-1/2/0.0
  Next hop: via so-5/1/0.0, selected
  Next hop: via so-6/0/0.0
  Protocol next hop: 172.23.2.129
  Indirect next hop: 89a1a00 264185
  State: <Active Ext>
  Local AS: 64500 Peer AS: 64490
  Age: 3:28 Metric: 0
  Task: BGP_64490.172.23.2.129+179
  Announcement bits (6): 0-KRT 1-RT 4-KRT 5-BGP.0.0.0.0+179

6-Resolve tree 2 7-Resolve tree 3
AS path: 64499 64510 645511 645511 645511 645511 645511 645511 I ( )
### show route damping history

```
user@host> show route damping history

inet.0: 173320 destinations, 1533529 routes (172624 active, 6 holddown, 108122 hidden)
+ = Active Route, - = Last Active, * = Both

10.108.0.0/15       [BGP] 2d 22:47:58, localpref 100
  AS path: 64220 65541 65542 I
  > to 192.168.60.85 via so-3/1/0.0
```

### show route damping history detail

```
user@host> show route damping history detail

inet.0: 173319 destinations, 1533435 routes (172627 active, 2 holddown, 108105 hidden)

10.108.0.0/15 (3 entries, 1 announced)
  BGP     /-101
  Next-hop reference count: 69058
  Source: 192.168.60.85
  Next hop: 192.168.60.85 via so-3/1/0.0, selected
  State: <Hidden Ext>
  Inactive reason: Unusable path
  Local AS: 64500 Peer AS: 64220
  Age: 2d 22:48:10
  Task: BGP_64220.192.168.60.85+179
  AS path: 64220 65541 65542 I ()
  Communities: 65541:390 65541:2000 65541:3000 65504:3561
  Localpref: 100
  Router ID: 192.168.80.25
  Merit (last update/now): 1000/932
  damping-parameters: set-normal
  Last update: 00:01:05 First update: 00:01:05
  Flaps: 1
```
**show route detail**

**List of Syntax**  
Syntax on page 2304  
Syntax (EX Series Switches) on page 2304

**Syntax**  
```
show route detail
<destination-prefix>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**  
```
show route detail
<destination-prefix>
```

**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 13.2X51-D15 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**  
Display detailed information about the active entries in the routing tables.

**Options**  
- `none`—Display all active entries in the routing table on all systems.  
  - `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**  
- `view`

**List of Sample Output**  
- show route detail on page 2315  
- show route detail (with BGP Multipath) on page 2321  
- show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2322  
- show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 2322  
- show route detail (Flexible VXLAN Tunnel Profile) on page 2323

**Output Fields**  
Table 171 on page 2304 describes the output fields for the `show route detail` command. Output fields are listed in the approximate order in which they appear.

**Table 171: show route detail Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td><code>number destinations</code></td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
</tbody>
</table>
### Table 171: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number routes</strong></td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• <strong>active</strong> (routes that are active)</td>
</tr>
<tr>
<td></td>
<td>• <strong>hold down</strong> (routes that are in the pending state before being declared inactive)</td>
</tr>
<tr>
<td></td>
<td>• <strong>hidden</strong> (routes that are not used because of a routing policy)</td>
</tr>
<tr>
<td><strong>route-destination</strong></td>
<td>Route destination (for example: 10.0.0.1/24). The <strong>entry</strong> value is the number of routes for this destination, and the <strong>announced</strong> value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td>• <strong>MPLS-label</strong> (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• <strong>interface-name</strong> (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address; control-word-status; encapsulation type; vc-id; source</strong> (Layer 2 circuit only; for example, 10.1.1.195: NoCtrlWord: 11: Local/96).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address</strong> — Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>control-word-status</strong> — Whether the use of the control word has been negotiated for this virtual circuit: <strong>NoCtrlWord</strong> or <strong>CtrlWord</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>encapsulation type</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vc-id</strong> — Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>• <strong>source</strong> — Source of the advertisement: <strong>Local</strong> or <strong>Remote</strong>.</td>
</tr>
<tr>
<td><strong>label stacking</strong></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>S=0 route</strong> indicates that a packet with an incoming label stack depth of 2 or more exits this routing device with one fewer label (the label-popping operation is performed).</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[protocol, preference]</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>Preference2 values are signed integers, that is, Preference2 values can be either positive or negative values. However, Junos OS evaluates Preference2 values as unsigned integers that are represented by positive values. Based on the Preference2 values, Junos OS evaluates a preferred route differently in the following scenarios:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>(IS-IS only). In IS-IS, a single 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.</td>
</tr>
<tr>
<td>PMSI</td>
<td>Provider multicast service interface (MVPN routing table).</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Next-hop type</td>
<td>Type of next hop. For a description of possible values for this field, see Table 172 on page 2310.</td>
</tr>
<tr>
<td>Next-hop reference count</td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td>Flood next-hop 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>
<tr>
<td>via</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Label-switched-path lsp-path-name</td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td>Label operation</td>
<td>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).</td>
</tr>
<tr>
<td>Interface</td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td>Protocol next hop</td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to derive a forwarding next hop.</td>
</tr>
<tr>
<td>Indirect next hop</td>
<td>Index designation used to specify the mapping between protocol next hops, tags, kernel export policy, and the forwarding next hops.</td>
</tr>
<tr>
<td>State</td>
<td>State of the route (a route can be in more than one state). See Table 173 on page 2312.</td>
</tr>
<tr>
<td>Local AS</td>
<td>AS number of the local routing device.</td>
</tr>
<tr>
<td>Age</td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td>AIGP</td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
</tbody>
</table>
### Table 171: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Metric</strong></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><strong>MED-plus-IGP</strong></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><strong>TTL-Action</strong></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. For sample output, see show route table.</td>
</tr>
<tr>
<td><strong>Task</strong></td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td><strong>Announcement bits</strong></td>
<td>The number of BGP peers or protocols to which Junos OS has announced this route, followed by the list of the recipients of the announcement. Junos OS can also announce the route to the KRT for installing the route into the Packet Forwarding Engine, to a resolve tree, a L2 VC, or even a VPN. For example, n-Resolve inet indicates that the specified route is used for route resolution for next hops found in the routing table.</td>
</tr>
<tr>
<td>• n</td>
<td>An index used by Juniper Networks customer support only.</td>
</tr>
<tr>
<td><strong>AS path</strong></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>• I</td>
<td>IGP.</td>
</tr>
<tr>
<td>• E</td>
<td>EGP.</td>
</tr>
<tr>
<td>• Recorded</td>
<td>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>When AS path numbers are included in the route, the format is as follows:</td>
<td></td>
</tr>
<tr>
<td>• [ ]</td>
<td>Brackets enclose the number that precedes the AS path. This number represents the number of ASs present in the AS path, when calculated as defined in RFC 4271. This value is used in the AS-path merge process, as defined in RFC 4893.</td>
</tr>
<tr>
<td>• [ ]</td>
<td>If more than one AS number is configured on the routing device, or if AS path prepending is configured, brackets enclose the local AS number associated with the AS path.</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>
</tbody>
</table>

**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.
### Table 171: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>validation-state</td>
<td>(BGP-learned routes) Validation status of the route:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid</strong>—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>• <strong>Unknown</strong>—Indicates that the prefix is not among the prefixes or prefix ranges in the database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unverified</strong>—Indicates that the origin of the prefix is not verified against the database. This is because the database got populated and the validation is not called for in the BGP import policy, although origin validation is enabled, or the origin validation is not enabled for the BGP peers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Valid</strong>—Indicates that the prefix and autonomous system pair are found in the database.</td>
</tr>
<tr>
<td>ORR Generation-ID</td>
<td>Displays the optimal route reflection (ORR) generation identifier. ISIS and OSPF interior gateway protocol (IGP) updates filed whenever any of the corresponding ORR route has its metric valued changed, or if the ORR route is added or deleted.</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>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>Prefixes bound to route</td>
<td>Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See Table 174 on page 2314 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>
</tbody>
</table>
Table 171: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<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>Accepted Multipath</td>
<td>Current active path when BGP multipath is configured.</td>
</tr>
<tr>
<td>Accepted LongLivedStale</td>
<td>The LongLivedStale flag indicates that the route was marked LLGR-stale by this router, as part of the operation of LLGR receiver mode. Either this flag or the LongLivedStaleImport flag may be displayed for a route. Neither of these flags are displayed at the same time as the Stale (ordinary GR stale) flag.</td>
</tr>
<tr>
<td>Accepted LongLivedStaleImport</td>
<td>The LongLivedStaleImport flag indicates that the route was marked LLGR-stale when it was received from a peer, or by import policy. Either this flag or the LongLivedStale flag may be displayed for a route. Neither of these flags are displayed at the same time as the Stale (ordinary GR stale) flag. Accept all received BGP long-lived graceful restart (LLGR) and LLGR stale routes learned from configured neighbors and import into the inet.0 routing table.</td>
</tr>
<tr>
<td>ImportAccepted LongLivedStaleImport</td>
<td>Accept all received BGP long-lived graceful restart (LLGR) and LLGR stale routes learned from configured neighbors and imported into the inet.0 routing table. The LongLivedStaleImport flag indicates that the route was marked LLGR-stale when it was received from a peer, or by import policy.</td>
</tr>
<tr>
<td>Accepted MultipathContrib</td>
<td>Path currently contributing to BGP multipath.</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 Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</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>
</tbody>
</table>

Table 172 on page 2310 describes all possible values for the Next-hop Types output field.

Table 172: Next-hop Types Output Field Values

<table>
<thead>
<tr>
<th>Next-Hop Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast (bcast)</td>
<td>Broadcast next hop.</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny next hop.</td>
</tr>
<tr>
<td>Discard</td>
<td>Discard next hop.</td>
</tr>
<tr>
<td>Dynamic List</td>
<td>Dynamic list next hop.</td>
</tr>
</tbody>
</table>
### Table 172: Next-hop Types Output Field Values (continued)

<table>
<thead>
<tr>
<th>Next-Hop Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flood</strong></td>
<td>Flood next hop. Consists of components called branches, up to a maximum of 32 branches. Each flood next-hop branch sends a copy of the traffic to the forwarding interface. Used by point-to-multipoint RSVP, point-to-multipoint LDP, point-to-multipoint CCC, and multicast.</td>
</tr>
<tr>
<td><strong>Hold</strong></td>
<td>Next hop is waiting to be resolved into a unicast or multicast type.</td>
</tr>
<tr>
<td><strong>Indexed (idxd)</strong></td>
<td>Indexed next hop.</td>
</tr>
<tr>
<td><strong>Indirect (indr)</strong></td>
<td>Used with applications that have a protocol next hop address that is remote. You are likely to see this next-hop type for internal BGP (IBGP) routes when the BGP next hop is a BGP neighbor that is not directly connected.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Used for a network address assigned to an interface. Unlike the router next hop, the interface next hop does not reference any specific node on the network.</td>
</tr>
<tr>
<td><strong>Local (local)</strong></td>
<td>Local address on an interface. This next-hop type causes packets with this destination address to be received locally.</td>
</tr>
<tr>
<td><strong>Multicast (mcst)</strong></td>
<td>Wire multicast next hop (limited to the LAN).</td>
</tr>
<tr>
<td><strong>Multicast discard (mdsc)</strong></td>
<td>Multicast discard.</td>
</tr>
<tr>
<td><strong>Multicast group (mgrp)</strong></td>
<td>Multicast group member.</td>
</tr>
<tr>
<td><strong>Receive (recv)</strong></td>
<td>Receive.</td>
</tr>
<tr>
<td><strong>Reject (rjct)</strong></td>
<td>Discard. An ICMP unreachable message was sent.</td>
</tr>
<tr>
<td><strong>Resolve (rlsv)</strong></td>
<td>Resolving next hop.</td>
</tr>
<tr>
<td><strong>Routed multicast (mcrt)</strong></td>
<td>Regular multicast next hop.</td>
</tr>
<tr>
<td><strong>Router</strong></td>
<td>A specific node or set of nodes to which the routing device forwards packets that match the route prefix. To qualify as next-hop type router, the route must meet the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• Must not be a direct or local subnet for the routing device.</td>
</tr>
<tr>
<td></td>
<td>• Must have a next hop that is directly connected to the routing device.</td>
</tr>
</tbody>
</table>
Table 172: Next-hop Types Output Field Values (continued)

<table>
<thead>
<tr>
<th>Next-Hop Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Next hop added to the Routing Engine forwarding table for remote IP addresses with prefix /32 for Junos OS Evolved only.</td>
</tr>
<tr>
<td>Table</td>
<td>Routing table next hop.</td>
</tr>
<tr>
<td>Unicast (ucst)</td>
<td>Unicast.</td>
</tr>
<tr>
<td>Unilist (ulst)</td>
<td>List of unicast next hops. A packet sent to this next hop goes to any next hop in the list.</td>
</tr>
</tbody>
</table>

Table 173 on page 2312 describes all possible values for the State output field. A route can be in more than one state (for example, `<Active NoReadvt Int Ext>`).

Table 173: State Output Field Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Route needs accounting.</td>
</tr>
<tr>
<td>Active</td>
<td>Route is active.</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>Clone</td>
<td>Route is a clone.</td>
</tr>
<tr>
<td>Cluster list length</td>
<td>Length of cluster list sent by the route reflector.</td>
</tr>
<tr>
<td>Delete</td>
<td>Route has been deleted.</td>
</tr>
<tr>
<td>Ex</td>
<td>Exterior route.</td>
</tr>
<tr>
<td>Ext</td>
<td>BGP route received from an external BGP neighbor.</td>
</tr>
<tr>
<td>FlashAll</td>
<td>Forces all protocols to be notified of a change to any route, active or inactive, for a prefix. When not set, protocols are informed of a prefix only when the active route changes.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Route not used because of routing policy.</td>
</tr>
<tr>
<td>IfCheck</td>
<td>Route needs forwarding RPF check.</td>
</tr>
</tbody>
</table>
Table 173: State Output Field Values (continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGP metric</td>
<td>Path through next hop with lower IGP metric is available.</td>
</tr>
<tr>
<td>Inactive reason</td>
<td>Flags for this route, which was not selected as best for a particular destination.</td>
</tr>
<tr>
<td>Initial</td>
<td>Route being added.</td>
</tr>
<tr>
<td>Int</td>
<td>Interior route.</td>
</tr>
<tr>
<td>Int Ext</td>
<td>BGP route received from an internal BGP peer or a BGP confederation peer.</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>Martian</td>
<td>Route is a martian (ignored because it is obviously invalid).</td>
</tr>
<tr>
<td>MartianOK</td>
<td>Route exempt from martian filtering.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Path with lower metric next hop is available.</td>
</tr>
<tr>
<td>No difference</td>
<td>Path from neighbor with lower IP address is available.</td>
</tr>
<tr>
<td>NoReadvrt</td>
<td>Route not to be advertised.</td>
</tr>
<tr>
<td>NotBest</td>
<td>Route not chosen because it does not have the lowest MED.</td>
</tr>
<tr>
<td>Not Best in its group</td>
<td>Incoming BGP AS is not the best of a group (only one AS can be the best).</td>
</tr>
<tr>
<td>NotInstall</td>
<td>Route not to be installed in the forwarding table.</td>
</tr>
<tr>
<td>Number of gateways</td>
<td>Path with a greater 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>Pending</td>
<td>Route pending because of a hold-down configured on another route.</td>
</tr>
<tr>
<td>Programmed</td>
<td>Route installed programatically by on-box or off-box applications using API.</td>
</tr>
<tr>
<td>Release</td>
<td>Route scheduled for release.</td>
</tr>
<tr>
<td>RIB preference</td>
<td>Route from a higher-numbered routing table is available.</td>
</tr>
</tbody>
</table>
Table 173: State Output Field Values (continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 lower preference value is available</td>
</tr>
<tr>
<td>Router ID</td>
<td>Path through a neighbor with lower ID is available.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Route not a primary route.</td>
</tr>
<tr>
<td>Unusable path</td>
<td>Path is not usable because of one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• The route is damped.</td>
</tr>
<tr>
<td></td>
<td>• The route is rejected by an import policy.</td>
</tr>
<tr>
<td></td>
<td>• The route is unresolved.</td>
</tr>
<tr>
<td>Update source</td>
<td>Last tiebreaker is the lowest IP address value.</td>
</tr>
<tr>
<td>ProtectionCand</td>
<td>Indicates paths requesting protection.</td>
</tr>
<tr>
<td>ProtectionPath</td>
<td>Indicates the route entry that can be used as a protection path.</td>
</tr>
</tbody>
</table>

Table 174 on page 2314 describes the possible values for the Communities output field.

Table 174: Communities Output Field Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-number</td>
<td>4 bytes, encoding a 32-bit area number. For AS-external routes, the value is 0. A nonzero value identifies the route as internal to the OSPF domain, and as within the identified area. Area numbers are relative to a particular OSPF domain.</td>
</tr>
<tr>
<td>bandwidth: local AS number:link-bandwidth-number</td>
<td>Link-bandwidth community value used for unequal-cost load balancing. When BGP has several candidate paths available for multipath purposes, it does not perform unequal-cost load balancing according to the link-bandwidth community unless all candidate paths have this attribute.</td>
</tr>
<tr>
<td>domain-id</td>
<td>Unique configurable number that identifies the OSPF domain.</td>
</tr>
<tr>
<td>domain-id-vendor</td>
<td>Unique configurable number that further identifies the OSPF domain.</td>
</tr>
<tr>
<td>link-bandwidth-number</td>
<td>Link-bandwidth number: from 0 through 4,294,967,295 (bytes per second).</td>
</tr>
<tr>
<td>local AS number</td>
<td>Local AS number: from 1 through 65,535.</td>
</tr>
<tr>
<td>options</td>
<td>1 byte. Currently this is only used if the route type is 5 or 7. Setting the least significant bit in the field indicates that the route carries a type 2 metric.</td>
</tr>
</tbody>
</table>
Table 174: Communities Output Field Values (continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>origin</td>
<td>(Used with VPNs) Identifies where the route came from.</td>
</tr>
<tr>
<td>ospf-route-type</td>
<td>1 byte, encoded as 1 or 2 for intra-area routes (depending on whether the route came from a type 1 or a type 2 LSA); 3 for summary routes; 5 for external routes (area number must be 0); 7 for NSSA routes; or 129 for sham link endpoint addresses.</td>
</tr>
<tr>
<td>route-type-vendor</td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x8000. The format is area-number: ospf-route-type: options.</td>
</tr>
<tr>
<td>rte-type</td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x0306. The format is area-number: ospf-route-type: options.</td>
</tr>
<tr>
<td>target</td>
<td>Defines which VPN the route participates in; target has the format 32-bit IP address: 16-bit number. For example, 10.19.0.0:100.</td>
</tr>
<tr>
<td>unknown IANA</td>
<td>Incoming IANA codes with a value between 0x1 and 0x7fff. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
<tr>
<td>unknown OSPF vendor community</td>
<td>Incoming IANA codes with a value above 0x8000. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
</tbody>
</table>

Sample Output

show route detail

user@host> show route detail

inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
  *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:  69
    Age: 1:31:43
    Task: RT
    Announcement bits (2): 0-KRT 3-Resolve tree 2
    AS path: I

10.31.1.0/30 (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:  69
    Age: 1:30:17
    Task: IF
    Announcement bits (1): 3-Resolve tree 2
AS path: I
OSP. Preference: 10
Next-hop reference count: 1
Next hop: via so-0/3/0.0, selected
State: <Int>
Inactive reason: Route Preference
Local AS: 69
Age: 1:30:17 Metric: 1
ORR Generation-ID: 1
Area: 0.0.0.0
Task: OSPF
AS path: I

10.31.1.1/32 (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: 69
  Age: 1:30:20
  Task: IF
  Announcement bits (1): 3-Resolve tree 2
  AS path: I

...
Chapter 25: Protocol-Independent Routing Operational Commands

Age: 1:31:43
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)

10.255.70.103/32 (1 entry, 1 announced)
   State: <FlashAll>
   *RSVP   Preference: 7
   Next-hop reference count: 6
   Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
   Label-switched-path green-r1-r3
   Label operation: Push 100096
   State: <Active Int>
   Local AS: 69
   Age: 1:25:49    Metric: 2
   Task: RSVP
   Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
   AS path: I

10.255.71.238/32 (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: 69
   Age: 1:25:49    Metric: 1
   Task: RSVP
   Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
   AS path: I

private__.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: 69
   Age: 1:31:44
   Task: IF
   AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
0  (1 entry, 1 announced)
   *MPLS Preference: 0
   Next hop type: Receive
   Next-hop reference count: 6
   State: <Active Int>
   Local AS: 69
   Age: 1:31:45    Metric: 1
   Task: MPLS
   Announcement bits (1): 0-KRT
   AS path: I
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

299840 (1 entry, 1 announced)
TSI:
KRT in-kernel 299840 /52 -> {indirect(1048575)}
   *RSVP   Preference: 7/2
   Next hop type: Flood
   Address: 0x9174a30
   Next-hop reference count: 4
   Next hop type: Router, Next hop index: 798
   Address: 0x9174c28
   Next-hop reference count: 2
   Next hop: 172.16.0.2 via lt-1/2/0.9 weight 0x1
   Label-switched-path R2-to-R4-2p2mp
   Label operation: Pop
   Next hop type: Router, Next hop index: 1048574
   Address: 0x92544f0
   Next-hop reference count: 2
   Next hop: 172.16.0.2 via lt-1/2/0.7 weight 0x1
   Label-switched-path R2-to-R200-p2mp
   Label operation: Pop
   Next hop: 172.16.0.2 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)
   VPLS   Preference: 7
   Next-hop reference count: 2
   Next hop: via vt-3/2/0.32769, selected
   Label operation: Pop
   State: <Active Int>
   Age: 1:29:30
   Task: Common L2 VC
   Announcement bits (1): 0-KRT
   AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)
   VPLS   Preference: 7
   Next-hop reference count: 2
   Next hop: 10.31.1.6 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: 10.255.70.103
   Push 800012
   Indirect next hop: 87272e4 1048574
   State: <Active Int>
   Age: 1:29:30
   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
inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

abcd::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: 69
  Age: 1:31:44
  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: 69
  Age: 1:31:44
  Task: IF
  AS path: I

ff02::2/128 (1 entry, 1 announced)
  *PIM Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:45
  Task: PIM Recv6
  Announcement bits (1): 0-KRT
  AS path: I

ff02::d/128 (1 entry, 1 announced)
  *PIM Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:45
  Task: PIM Recv6
  Announcement bits (1): 0-KRT
  AS path: I

ff02::16/128 (1 entry, 1 announced)
  *MLD Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:43
  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: 1:31:44
Task: IF
AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS:  69 Peer AS:  69
  Age: 1:25:49  Metric2: 1
  AIGP 210
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-green-l2vpn
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 100
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
  *L2VPN  Preference: 170/-1
  Next-hop reference count: 5
  Protocol next hop: 10.255.71.52
  Indirect next hop: 0 -
  State: <Active Int Ext>
  Age: 1:31:40  Metric2: 1
  Task: green-l2vpn
  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

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
  *L2VPN  Preference: 170/-101
  Next-hop reference count: 5
  Protocol next hop: 10.255.71.52
  Indirect next hop: 0 -
  State: <Active Int Ext>
  Age: 1:31:40  Metric2: 1
  Task: green-l2vpn
  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

...
"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 circuit
Announcement bits (1): 0-LDP
AS path: I
VC Label 100000, MTU 1500, VLAN ID 512
inet.0: 45 destinations, 47 routes (44 active, 0 holddown, 1 hidden)
1.1.1.3/32 (1 entry, 1 announced)
*IS-IS Preference: 18
Level: 2
Next hop type: Router, Next hop index: 580
Address: 0x9db6ed0
Next-hop reference count: 8
Next hop: 10.1.1.6 via lt-1/0/10.5, selected
Session Id: 0x18a
State: <Active Int>
Local AS: 2
Age: 1:32 Metric: 10
Validation State: unverified
ORR Generation-ID: 1
Task: IS-IS
Announcement bits (3): 0-KRT 5-Resolve tree 4 6-Resolve_I GP_FRR
inet.0: 61 destinations, 77 routes (61 active, 1 holddown, 0 hidden)
1.1.1.1/32 (2 entries, 1 announced)
*OSPF Preference: 10
Next hop type: Router, Next hop index: 673
Address: 0xc008830
Next-hop reference count: 3
Next hop: 10.1.1.1 via ge-0/0/2.0, selected
Session Id: 0x1b7
State: <Active Int>
Local AS: 1
Age: 3:06:59 Metric: 100
Validation State: unverified
ORR Generation-ID: 1
Area: 0.0.0.0
Task: OSPF
Announcement bits (2): 1-KRT 9-Resolve tree 2
AS path: I

show route detail (with BGP Multipath)

user@host> show route detail

10.1.1.8/30 (2 entries, 1 announced)
*BGP Preference: 170/-101
Next hop type: Router, Next hop index: 262142
Address: 0x901a010
Next-hop reference count: 2
Source: 10.1.1.2
Next hop: 10.1.1.2 via ge-0/3/0.1, selected
Next hop: 10.1.1.6 via ge-0/3/0.5
State: <Active Ext>
Local AS:     1 Peer AS:     2
Age: 5:04:43
Validation State: unverified
Task: BGP_2.10.1.1.2+59955
Announcement bits (1): 0-KRT
AS path: 2 I
Accepted Multipath
Localpref: 100
Router ID: 172.16.1.2
BGP Preference: 170/-101
Next hop type: Router, Next hop index: 678
Address: 0x8f97520
Next-hop reference count: 9
Source: 10.1.1.6
Next hop: 10.1.1.6 via ge-0/3/0.5, selected
State: <NotBest Ext>
Inactive reason: Not Best in its group - Active preferred
Local AS:     1 Peer AS:     2
Age: 5:04:43
Validation State: unverified
Task: BGP_2.10.1.1.6+58198
AS path: 2 I
Accepted MultipathContrib
Localpref: 100
Router ID: 172.16.1.3

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:  1001
    Age: 8:20       Metric: 1
    Task: LDP
    Announcement bits (1): 0-KRT
    AS path: I
    FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1, 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: 1.3.8.2 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: 1.3.4.2 via ge-1/2/18.0
  Label operation: Pop
  Load balance label: None;
  State: <Active Int AckRequest MulticastRPF>
  Local AS:    10
  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 172.16.1.1, grp: 232.1.1.1,
  src: 192.168.219.11
  Primary Upstream : 172.16.1.3:0--172.16.1.2:0
  RPF Nexthops :
    ge-1/2/15.0, 1.2.94.1, Label: 301568, weight: 0x1
    ge-1/2/14.0, 1.2.3.1, Label: 301568, weight: 0x1
  Backup Upstream : 172.16.1.3:0--172.16.1.6:0
  RPF Nexthops :
    ge-1/2/20.0, 1.2.96.1, Label: 301584, weight: 0xffff
    ge-1/2/19.0, 1.3.6.1, Label: 301584, weight: 0xffff

show route detail (Flexible VXLAN Tunnel Profile)

user@host> show route 192.168.0.2 detail

...  
CUSTOMER_0001.inet.0: 5618 destinations, 6018 routes (5618 active, 0 holddown, 0 hidden)

192.168.0.2/32 (1 entry, 1 announced)
  *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: 1:25:53
  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 exact**

**List of Syntax**  
Syntax on page 2325  
Syntax (EX Series Switches) on page 2325

**Syntax**  
show route exact destination-prefix  
<brief | detail | extensive | terse>  
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches)**  
show route exact destination-prefix  
<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.

**Description**  
Display only the routes that exactly match the specified address or range of addresses.

**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.

destination-prefix—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**  
view

**List of Sample Output**  
show route exact on page 2325  
show route exact detail on page 2326  
show route exact extensive on page 2326  
show route exact terse on page 2326

**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 exact

```
user@host> show route exact 207.17.136.0/24

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
```
show route exact detail

user@host> show route exact 207.17.136.0/24 detail

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
207.17.136.0/24 (1 entry, 1 announced)
  *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:    69
  Age: 2d 3:30:26
  Task: RT
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

show route exact extensive

user@host> show route exact 207.17.136.0/24 extensive

inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
207.17.136.0/24 (1 entry, 1 announced)
TSI:
KRT in-kernel 207.17.136.0/24 -> {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:    69
  Age: 1:25:18
  Task: RT
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

show route exact terse

user@host> show route exact 207.17.136.0/24 terse

inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
A Destination P Prf Metric 1 Metric 2 Next hop AS path
* 207.17.136.0/24 S      5 >192.168.71.254
**show route export**

**List of Syntax**  
Syntax on page 2327  
Syntax (EX Series Switches) on page 2327

**Syntax**  
`show route export`  
`<brief | detail>`  
`<instance <instance-name> | routing-table-name>`  
`<logical-system (all | logical-system-name)>`

**Syntax (EX Series Switches)**  
`show route export`  
`<brief | detail>`  
`<instance <instance-name> | routing-table-name>`

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

**Description**  
Display policy-based route export information. Policy-based export simplifies the process of exchanging route information between routing instances.

**Options**  
`none`—(Same as `brief`.) Display standard information about policy-based export for all instances and routing tables on all systems.  
`brief | detail`—(Optional) Display the specified level of output.  
`instance <instance-name>`—(Optional) Display a particular routing instance for which policy-based export is currently enabled.  
`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.  
`routing-table-name`—(Optional) Display information about policy-based export for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the `show route export inet` command).

**Required Privilege Level**  
`view`

**List of Sample Output**  
show route export on page 2328  
show route export detail on page 2328  
show route export instance detail on page 2329

**Output Fields**  
Table 175 on page 2328 lists the output fields for the `show route export` command. Output fields are listed in the approximate order in which they appear.
### Table 175: show route export Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table or table-name</td>
<td>Name of the routing tables that either import or export routes.</td>
<td>All levels</td>
</tr>
<tr>
<td>Routes</td>
<td>Number of routes exported from this table into other tables. If a particular route is exported to different tables, the counter will only increment by one.</td>
<td>brief none</td>
</tr>
<tr>
<td>Export</td>
<td>Whether the table is currently exporting routes to other tables: Y or N (Yes or No).</td>
<td>brief none</td>
</tr>
<tr>
<td>Import</td>
<td>Tables currently importing routes from the originator table. (Not displayed for tables that are not exporting any routes.)</td>
<td>detail</td>
</tr>
<tr>
<td>Flags</td>
<td>(instance keyword only) Flags for this feature on this instance:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• config auto-policy—The policy was deduced from the configured IGP export policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• cleanup—Configuration information for this instance is no longer valid.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• config—The instance was explicitly configured.</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>(instance keyword only) Configured option displays the type of routing tables the feature handles:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• unicast—Indicates instance.inet.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast—Indicates instance.inet.2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unicast multicast—Indicates instance.inet.0 and instance.inet.2.</td>
<td></td>
</tr>
<tr>
<td>Import policy</td>
<td>(instance keyword only) Policy that route export uses to construct the import-export matrix. Not displayed if the instance type is vrf.</td>
<td>detail</td>
</tr>
<tr>
<td>Instance</td>
<td>(instance keyword only) Name of the routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>(instance keyword only) Type of routing instance: forwarding, non-forwarding, or vrf.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

**show route export**

```bash
user@host> show route export
```

<table>
<thead>
<tr>
<th>Table</th>
<th>Export</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet.0</td>
<td>N</td>
<td>0</td>
</tr>
<tr>
<td>black.inet.0</td>
<td>Y</td>
<td>3</td>
</tr>
<tr>
<td>red.inet.0</td>
<td>Y</td>
<td>4</td>
</tr>
</tbody>
</table>

**show route export detail**

```bash
user@host> show route export detail
```

<table>
<thead>
<tr>
<th>Table</th>
<th>Routes:</th>
<th>Routes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet.0</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>black.inet.0</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Import: [inet.0]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show route export instance detail

user@host> show route export instance detail

<table>
<thead>
<tr>
<th>Instance</th>
<th>Type</th>
<th>Flags</th>
<th>Options</th>
<th>Import policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>forwarding</td>
<td>&lt;config auto-policy&gt;</td>
<td>&lt;unicast multicast&gt;</td>
<td>(ospf-master-from-red</td>
</tr>
<tr>
<td>black</td>
<td>non-forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>red</td>
<td>non-forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show route export vrf-target**

**Syntax**

```
show route export vrf-target
  <brief | detail>
  <community community--regular-expression>
  <logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

Display the VPN routing and forwarding (VRF) target communities for which policy-based route export is currently distributing routes. This command is relevant when there are overlapping virtual private networks (VPNs).

**Options**

- **none**—Display standard information about all target communities.
- **brief | detail**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.
- **community community--regular-expression**—(Optional) Display information about the specified community.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

view

**List of Sample Output**

- show route export vrf-target on page 2331
- show route export vrf-target community on page 2331
- show route export vrf-target detail on page 2331

**Output Fields**

Table 176 on page 2330 lists the output fields for the `show route export vrf-target` 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>Route target</td>
<td>Target communities for which auto-export is currently distributing routes.</td>
<td>brief none</td>
</tr>
<tr>
<td>Family</td>
<td>Routing table entries for the specified family.</td>
<td>brief none</td>
</tr>
<tr>
<td>type-of-routing-table(s)</td>
<td>Type of routing tables the feature handles:</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>• unicast—Indicates instance.inet.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast—Indicates instance.inet.2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unicast multicast—Indicates instance.inet.0 and instance.inet.2.</td>
<td></td>
</tr>
</tbody>
</table>
Table 176: show route export vrf-target 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>Import</strong></td>
<td>Number of routing tables that are currently importing routes with this target</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>community. Omitted for tables that are not importing routes.</td>
<td></td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Number of routing tables that are currently exporting routes with this target</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>community. Omitted for tables that are not exporting routes.</td>
<td></td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Target communities, family, and options for which auto-export is currently</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>distributing routes.</td>
<td></td>
</tr>
<tr>
<td><strong>Import table(s)</strong></td>
<td>Name of the routing tables that are importing a particular route target.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Export table(s)</strong></td>
<td>Name of the routing tables that are exporting a particular route target.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

**show route export vrf-target**

```
user@host> show route export vrf-target

Route Target             Family                  Import     Export
 69:1                     inet     unicast             2          2
 69:2                     inet     unicast             2          2
```

**show route export vrf-target community**

```
user@host> show route export vrf-target community target:69:1

Route Target             Family                  Import     Export
 69:1                     inet     unicast             2          2
```

**show route export vrf-target detail**

```
user@host> show route export vrf-target detail

Target: 1:12: inet     unicast
  Import table(s): vrf-11.inet.0  vrf-12.inet.0
  Export table(s): vrf-12.inet.0

Target: 1:13: inet     unicast
  Import table(s): vrf-12.inet.0  vrf-13.inet.0
  Export table(s): vrf-13.inet.0
```
show route extensive

List of Syntax  Syntax on page 2332
Syntax (EX Series Switches) on page 2332

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  view

List of Sample Output  show route extensive on page 2339
show route extensive (Access Route) on page 2346
show route extensive (BGP PIC Edge) on page 2347
show route extensive (FRR and LFA) on page 2347
show route extensive (IS-IS) on page 2348
show route extensive (Route Reflector) on page 2348
show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2349
show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 2349
show route extensive (Flexible VXLAN Tunnel Profile) on page 2350

Output Fields  Table 177 on page 2332 describes the output fields for the show route extensive command. Output fields are listed in the approximate order in which they appear.

Table 177: 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>
</tbody>
</table>
### Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>- active (routes that are active).</td>
</tr>
<tr>
<td></td>
<td>- holdown (routes that are in the pending state before being declared inactive).</td>
</tr>
<tr>
<td></td>
<td>- hidden (routes that are not used because of a routing policy).</td>
</tr>
<tr>
<td>route-destination</td>
<td>Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination,</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td>and the announced value is the number of routes being announced for this destination. Sometimes the route</td>
</tr>
<tr>
<td></td>
<td>destination is presented in another format, such as:</td>
</tr>
<tr>
<td></td>
<td>- MPLS-label (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>- interface-name (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>- neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only; for example,</td>
</tr>
<tr>
<td></td>
<td>- neighbor-address—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>- control-word-status—Whether the use of the control word has been negotiated for this virtual circuit:</td>
</tr>
<tr>
<td></td>
<td>NoCtrlWord or CtrlWord.</td>
</tr>
<tr>
<td></td>
<td>- encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5</td>
</tr>
<tr>
<td></td>
<td>VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8)</td>
</tr>
<tr>
<td></td>
<td>ATM VCC cell transport, (10) ATM VPC cell transport.</td>
</tr>
<tr>
<td></td>
<td>- vc-id—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>- source—Source of the advertisement: Local or Remote.</td>
</tr>
<tr>
<td>TSI</td>
<td>Protocol header information.</td>
</tr>
<tr>
<td>label stacking</td>
<td>(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping</td>
</tr>
<tr>
<td></td>
<td>operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed,</td>
</tr>
<tr>
<td></td>
<td>because the pop operation is performed only when the stack depth is two or more labels.</td>
</tr>
<tr>
<td></td>
<td>- S=Route indicates that a packet with an incoming label stack depth of two or more exits this router with</td>
</tr>
<tr>
<td></td>
<td>one fewer label (the label-popping operation is performed).</td>
</tr>
<tr>
<td></td>
<td>- If there is no S= information, the route is a normal MPLS route, which has a stack depth of 1 (the</td>
</tr>
<tr>
<td></td>
<td>label-popping operation is not performed).</td>
</tr>
<tr>
<td>[protocol, preference]</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>- +—A plus sign indicates the active route, which is the route installed from the routing table into the</td>
</tr>
<tr>
<td></td>
<td>forwarding table.</td>
</tr>
<tr>
<td></td>
<td>- -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>- *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a</td>
</tr>
<tr>
<td></td>
<td>to line indicates the best subpath to the route.</td>
</tr>
</tbody>
</table>

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.
Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>(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.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>IP subnet augmented with a 64-bit prefix.</td>
</tr>
<tr>
<td>PMSI</td>
<td>Provider multicast service interface (MVPN routing table).</td>
</tr>
<tr>
<td>Next-hop type</td>
<td>Type of next hop. For a description of possible values for this field, see the Output Field table in the show route detail command.</td>
</tr>
<tr>
<td>Next-hop reference count</td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td>Flood next-hop 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>
<tr>
<td>via</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Label-switched-path</td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td>lsp-path-name</td>
<td></td>
</tr>
<tr>
<td>Label operation</td>
<td>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).</td>
</tr>
<tr>
<td>Offset</td>
<td>Whether the metric has been increased or decreased by an offset value.</td>
</tr>
<tr>
<td>Interface</td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td>Protocol next hop</td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.</td>
</tr>
</tbody>
</table>
### Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>label-operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
</tbody>
</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 177: 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></td>
<td>• Active preferred—Currently active route was selected over this route.</td>
</tr>
<tr>
<td></td>
<td>• Always compare MED—Path with a lower multiple exit discriminator (MED) is available.</td>
</tr>
<tr>
<td></td>
<td>• AS path—Shorter AS path is available.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Non-deterministic MED selection—Cisco nondeterministic MED is enabled and a path with a lower MED is available.</td>
</tr>
<tr>
<td></td>
<td>• Cluster list length—Path with a shorter cluster list length is available.</td>
</tr>
<tr>
<td></td>
<td>• Forwarding use only—Path is only available for forwarding purposes.</td>
</tr>
<tr>
<td></td>
<td>• IGP metric—Path through the next hop with a lower IGP metric is available.</td>
</tr>
<tr>
<td></td>
<td>• IGP metric type—Path with a lower OSPF link-state advertisement type is available.</td>
</tr>
<tr>
<td></td>
<td>• Interior &gt; Exterior &gt; Exterior via Interior—Direct, static, IGP, or EBGP path is available.</td>
</tr>
<tr>
<td></td>
<td>• Local preference—Path with a higher local preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• Next hop address—Path with a lower metric next hop is available.</td>
</tr>
<tr>
<td></td>
<td>• No difference—Path from a neighbor with a lower IP address is available.</td>
</tr>
<tr>
<td></td>
<td>• Not Best in its group—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></td>
<td>• Number of gateways—Path with a higher number of next hops is available.</td>
</tr>
<tr>
<td></td>
<td>• Origin—Path with a lower origin code is available.</td>
</tr>
<tr>
<td></td>
<td>• OSPF version—Path does not support the indicated OSPF version.</td>
</tr>
<tr>
<td></td>
<td>• RIB preference—Route from a higher-numbered routing table is available.</td>
</tr>
<tr>
<td></td>
<td>• Route destinguisher—64-bit prefix added to IP subnets to make them unique.</td>
</tr>
<tr>
<td></td>
<td>• Route metric or MED comparison—Route with a lower metric or MED is available.</td>
</tr>
<tr>
<td></td>
<td>• Route preference—Route with a lower preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• Router ID—Path through a neighbor with a lower ID is available.</td>
</tr>
<tr>
<td></td>
<td>• Unusable path—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></td>
<td>• Update source—Last tiebreaker is the lowest IP address value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Local AS</strong></th>
<th>Autonomous system (AS) number of the local routing device.</th>
</tr>
</thead>
<tbody>
<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><strong>Metric</strong></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><strong>MED-plus-IGP</strong></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><strong>TTL-Action</strong></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>
</tbody>
</table>

For sample output, see `show route table`. 
## Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
</tbody>
</table>
| Announcement bits| List of protocols that are consumers of the route. Using the following output as an example, Announcement bits (3): 0-KRT 5-Resolve tree 2 BGP RT Background 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).

The notation n-Resolve inet indicates that the route is used for route resolution for next hops found in the routing table. n is an index used by Juniper Networks customer support only.

### AS path

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:

- I—IGP.
- E—EGP.
- Recorded—The AS path is recorded by the sample process (sampled).
- ?—Incomplete; typically, the AS path was aggregated.

When AS path numbers are included in the route, the format is as follows:

- [ ]—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.
- { }—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.
- ()—Parentheses enclose a confederation.
- ( [ ])—Parentheses and brackets enclose a confederation set.

**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.

### validation-state

(BGP-learned routes) Validation status of the route:

- 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.
- Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database.
- Unverified—Indicates that origin validation is not enabled for the BGP peers.
- Valid—Indicates that the prefix and autonomous system pair are found in the database.

### FECs bound to route

Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.

### AS path: I <Originator>

(For route reflected output only) Originator ID attribute set by the route reflector.
### Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>route status</strong></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>
</tbody>
</table>

- **Primary Upstream**: 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.

- **RPF Nexthops**: 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.

- **Label**: 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.

- **weight**: 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.

- **VC Label**: MPLS label assigned to the Layer 2 circuit virtual connection.

- **MTU**: Maximum transmission unit (MTU) of the Layer 2 circuit.

- **VLAN ID**: VLAN identifier of the Layer 2 circuit.

- **Cluster list**: (For route reflected output only) Cluster ID sent by the route reflector.

- **Originator ID**: (For route reflected output only) Address of router that originally sent the route to the route reflector.

- **Prefixes bound to route**: Forwarding Equivalent Class (FEC) bound to this route. Applicable only to routes installed by LDP.

- **Communities**: Community path attribute for the route. See the Output Field table in the `show route detail` command for all possible values for this field.

- **Layer2-info: encaps**: Layer 2 encapsulation (for example, VPLS).

- **control flags**: Control flags: `none` or Site Down.

- **mtu**: Maximum transmission unit (MTU) information.

- **Label-Base, range**: 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.
Table 177: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<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 Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</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
```

Chapter 25: Protocol-Independent Routing Operational Commands

Copyright © 2019, Juniper Networks, Inc.
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: 64496
  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

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299840 (1 entry, 1 announced)

TSI:
KRT in-kernel 299840 /52 -> {indirect(1048575)}
  *RSVP  Preference: 7/2
    Next hop type: Flood
    Address: 0x9174a30
    Next-hop reference count: 4
    Next hop type: Router, Next hop index: 798
    Address: 0x9174c28
    Next-hop reference count: 2
    Next hop: 198.51.100.2 via lt-1/2/0.9 weight 0x1
    Label-switched-path R2-to-R4-2p2mp
    Label operation: Pop
    Next hop type: Router, Next hop index: 1048574
    Address: 0x92544f0
    Next-hop reference count: 2
    Next hop: 198.51.100.2 via lt-1/2/0.7 weight 0x1
    Label-switched-path R2-to-R200-p2mp
    Label operation: Pop
    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-l2vpn
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.l2vpn.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-l2vpn
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-l2vpn
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: l2 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
Localpref: 100
Router ID: 213.0.113.99

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
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
    Age: 25
    Metric2: 15
    Validation State: unverified
    Task: RT
    Announcement bits (1): 0-KRT
    AS path: 3 I
    Communities: target:2:1

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: 1048574
    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
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: 0xYYYYYYYYYY
Next-hop reference count: YY
Next hop: 203.0.113.22 via ae0.0 balance 57%
Session Id: 0x141

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: 65544 64500 65548
  Cluster list: 198.51.100.1
  Originator ID: 203.0.113.88
  Communities: 7777:7777
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
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 flow validation

List of Syntax  Syntax on page 2351
Syntax (EX Series Switches) on page 2351

Syntax  show route flow validation
  <brief | detail>
  <ip-prefix>
  <table table-name>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route flow validation
  <brief | detail>
  <ip-prefix>
  <table table-name>

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

Description  Display flow route information.

Options  none—Display flow route information.
  brief | detail—(Optional) Display the specified level of output. If you do not specify a
  level of output, the system defaults to brief.
  ip-prefix—(Optional) IP address for the flow route.
  logical-system (all | logical-system-name)—(Optional) Perform this operation on all
  logical systems or on a particular logical system.
  table table-name—(Optional) Display flow route information for all routing tables whose
  name begins with this string (for example, inet.0 and inet6.0 are both displayed
  when you run the show route flow validation inet command).

Required Privilege  view

List of Sample Output  show route flow validation on page 2352
show route flow validation (IPv6) on page 2352

Output Fields  Table 178 on page 2352 lists the output fields for the show route flow validation command. Output fields are listed in the approximate order in which they appear.
Table 178: show route flow validation Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, inet.0).</td>
<td>All levels</td>
</tr>
<tr>
<td>prefix</td>
<td>Route address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Active unicast route</td>
<td>Active route in the routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Dependent flow destinations</td>
<td>Number of flows for which there are routes in the routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Origin</td>
<td>Source of the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor AS</td>
<td>Autonomous system identifier of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow destination</td>
<td>Number of entries and number of destinations that match the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unicast best match</td>
<td>Destination that is the best match for the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the route flow.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show route flow validation

user@host> show route flow validation
inet.0:
  10.0.5.0/24 Active unicast route
  Dependent flow destinations: 1
  Origin: 192.168.224.218, Neighbor AS: 64501
  Flow destination (3 entries, 1 match origin)
  Unicast best match: 10.0.5.0/24
  Flags: SubtreeApex Consistent

show route flow validation (IPv6)

user@host> show route flow validation
inet6.0:
  2001:db8::11:11:11:0/120
    Active unicast route
    Dependent flow destinations: 2
  2001:db8::11:11:11:10/128
    Flow destination (1 entries, 1 match origin, next-as)
    Unicast best match: 2001:db8::11:11:11:0/120
    Flags: Consistent
  2001:db8::11:11:11:30/128
    Flow destination (1 entries, 1 match origin, next-as)
<table>
<thead>
<tr>
<th>Unicast best match: 2001:db8::11:11:0/120</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: Consistent</td>
</tr>
</tbody>
</table>
show route forwarding-table

<table>
<thead>
<tr>
<th>List of Syntax</th>
<th>Syntax on page 2354</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Syntax (MX Series Routers) on page 2354</td>
</tr>
<tr>
<td></td>
<td>Syntax (TX Matrix and TX Matrix Plus Routers) on page 2354</td>
</tr>
</tbody>
</table>

Syntax  
```
show route forwarding-table
<detail | extensive | summary>
<all>
<ccc interface-name>
<destination destination-prefix>
?family family | matching matching>
<interface-name interface-name>
<label name>
<matching matching>
<multicast>
<table (default | logical-system-name/routing-instance-name | routing-instance-name)>
<vlan (all | vlan-name)>
<vpn vpn>
```

Syntax (MX Series Routers)  
```
show route forwarding-table
<detail | extensive | summary>
<all>
<bridge-domain (all | domain-name)>
<ccc interface-name>
<destination destination-prefix>
?family family | matching matching>
<interface-name interface-name>
<label name>
<learning-vlan-id learning-vlan-id>
<matching matching>
<multicast>
<table (default | logical-system-name/routing-instance-name | routing-instance-name)>
<vlan (all | vlan-name)>
<vpn vpn>
```

Syntax (TX Matrix and TX Matrix Plus Routers)  
```
show route forwarding-table
<detail | extensive | summary>
<all>
<ccc interface-name>
<destination destination-prefix>
?family family | matching matching>
<interface-name interface-name>
<matching matching>
<label name>
<lcc number>
<multicast>
<table routing-instance-name>
<vpn vpn>
```
**Release Information**  
Command introduced before Junos OS Release 7.4.  
Option `bridge-domain` introduced in Junos OS Release 7.5  
Option `learning-vlan-id` introduced in Junos OS Release 8.4  
Options `all` and `vlan` introduced in Junos OS Release 9.6.  
Command introduced in Junos OS Release 11.3 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**  
Display the Routing Engine's forwarding table, including the network-layer prefixes and their next hops. This command is used to help verify that the routing protocol process has relayed the correction information to the forwarding table. The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the forwarding table.

---

**NOTE:** The Routing Engine copies the forwarding table to the Packet Forwarding Engine, the part of the router that is responsible for forwarding packets. To display the entries in the Packet Forwarding Engine's forwarding table, use the `show pfe route` command.

---

**Options**

- `none`—Display the routes in the forwarding tables. By default, the `show route forwarding-table` command does not display information about private, or internal, forwarding tables.

- `detail | extensive | summary`—(Optional) Display the specified level of output.

- `all`—(Optional) Display routing table entries for all forwarding tables, including private, or internal, tables.

- `bridge-domain (all | bridge-domain-name)`—(MX Series routers only) (Optional) Display route entries for all bridge domains or the specified bridge domain.

- `ccc interface-name`—(Optional) Display route entries for the specified circuit cross-connect interface.

- `destination destination-prefix`—(Optional) Destination prefix.

- `family family`—(Optional) Display routing table entries for the specified family: `bridge (ccc | destination | detail | extensive | interface-name | label | learning-vlan-id | matching | multicast | summary | table | vlan | vpn), ethernet-switching, evpn, fibre-channel, fmembers, inet, inet6, iso, mcsnoop-inet, mcsnoop-inet6, mpls, satellite-inet, satellite-inet6, satellite-vpls, tnp, unix, vpls, or vlan-classification`.

- `interface-name interface-name`—(Optional) Display routing table entries for the specified interface.

- `label name`—(Optional) Display route entries for the specified label.

- `lcc number`—(TX Matrix and TX matrix Plus routers only) (Optional) On a routing matrix composed of a TX Matrix router and T640 routers, display information for the
specified T640 router (or line-card chassis) connected to the TX Matrix router. On a routing matrix composed of the TX Matrix Plus router and T1600 or T4000 routers, display information for the specified router (line-card chassis) 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.

**learning-vlan-id**—(MX Series routers only) (Optional) Display learned information for all VLANs or for the specified VLAN.

**matching**—(Optional) Display routing table entries matching the specified prefix or prefix length.

**multicast**—(Optional) Display routing table entries for multicast routes.

**table**—(Optional) Display route entries for all the routing tables in the main routing instance or for the specified routing instance. If your device supports logical systems, you can also display route entries for the specified logical system and routing instance. To view the routing instances on your device, use the `show route instance` command.

**vlan (all | vlan-name)**—(Optional) Display information for all VLANs or for the specified VLAN.

**vpn vpn**—(Optional) Display routing table entries for a specified VPN.

<table>
<thead>
<tr>
<th>Required Privilege</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
<td></td>
</tr>
</tbody>
</table>

**List of Sample Output**

- show route forwarding-table on page 2361
- show route forwarding-table detail on page 2362
- show route forwarding-table destination extensive (Weights and Balances) on page 2362
- show route forwarding-table extensive on page 2363
- show route forwarding-table extensive (RPF) on page 2364
- show route forwarding-table extensive (PIM using point-to-multipoint mode) on page 2365
- show route forwarding-table (dynamic list next hop) on page 2365
- show route forwarding-table family mpls on page 2366
- show route forwarding-table family mpls ccc ge-0/0/1.1004 on page 2366
- show route forwarding-table family vpls on page 2367
show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled) on page 2367
show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled with MAC Statistics) on page 2367
show route forwarding-table family vpls extensive on page 2368
show route forwarding-table table default on page 2369
show route forwarding-table table logical-system-name/routing-instance-name on page 2370
show route forwarding-table vpn on page 2371

Output Fields
Table 179 on page 2357 lists the output fields for the show route forwarding-table command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified, or when the detail keyword is used instead of the extensive keyword.

Table 179: show route forwarding-table Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical system</td>
<td>Name of the logical system. This field is displayed if you specify the table logical-system-name/routing-instance-name option on a device that is configured for and supports logical systems.</td>
<td>All levels</td>
</tr>
<tr>
<td>Routing table</td>
<td>Name of the routing table (for example, inet, inet6, mpls).</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 179: show route forwarding-table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled protocols</td>
<td>The features and protocols that have been enabled for a given routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>This field can contain the following values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BUM hashing—BUM hashing is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC Stats—Mac Statistics is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bridging—Routing instance is a normal layer 2 bridge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No VLAN—No VLANs are associated with the bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All VLANs—The <code>vlan-id all</code> statement has been enabled for this bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Single VLAN—Single VLAN ID is associated with the bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC action drop—New MACs will be dropped when the MAC address limit is reached.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dual VLAN—Dual VLAN tags are associated with the bridge domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No local switching—No local switching is enabled for this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Learning disabled—Layer 2 learning is disabled for this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC limit reached—The maximum number of MAC addresses that was configured for this routing instance has been reached.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VPLS—The VPLS protocol is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No IRB l2-copy—The no-irb-layer-2-copy feature is enabled for this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ACKed by all peers—All peers have acknowledged this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BUM Pruning—BUM pruning is enabled on the VPLS instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Def BD VXLAN—VXLAN is enabled for the default bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EVPN—EVPN protocol is enabled for this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Def BD OVSDB—Open vSwitch Database (OVSDB) is enabled on the default bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Def BD Ingress replication—VXLAN ingress node replication is enabled on the default bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L2 backhaul—Layer 2 backhaul is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FRR optimize—Fast reroute optimization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC pinning—MAC pinning is enabled for this bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC Aging Timer—The MAC table aging time is set per routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EVPN VXLAN—This routing instance supports EVPN with VXLAN encapsulation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PBBN—This routing instance is configured as a provider backbone bridged network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PBN—This routing instance is configured as a provider bridge network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ETREE—The ETREE protocol is enabled on this EVPN routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ARP/NDP suppression—EVPN ARP NDP suppression is enabled in this routing instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Def BEVPN VXLAN—EVPN VXLAN is enabled for the default bridge domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MPLS control word—Control word is enabled for this MPLS routing instance.</td>
<td></td>
</tr>
<tr>
<td>Address family</td>
<td>Address family (for example, IP, IPv6, ISO, MPLS, and VPLS).</td>
<td>All levels</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination of the route.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 179: show route forwarding-table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| Route Type (Type)   | How the route was placed into the forwarding table. When the `detail` keyword is used, the route type might be abbreviated (as shown in parentheses):
  - `cloned (clon)`—(TCP or multicast only) Cloned route.                                    | All levels      |
  - `destination (dest)`—Remote addresses directly reachable through an interface.            |                 |
  - `destination down (iddn)`—Destination route for which the interface is unreachable.       |                 |
  - `interface cloned (ifcl)`—Cloned route for which the interface is unreachable.           |                 |
  - `route down (ifdn)`—Interface route for which the interface is unreachable.               |                 |
  - `ignore (ignr)`—Ignore this route.                                                       |                 |
  - `interface (intf)`—Installed as a result of configuring an interface.                     |                 |
  - `permanent (perm)`—Routes installed by the kernel when the routing table is initialized. |                 |
  - `user`—Routes installed by the routing protocol process or as a result of the configuration. |                 |
| Route Reference (RtRef) | Number of routes to reference.                                                                                                                                                                                             | `detail extensive` |
| Flags               | Route type flags:                                                                                                                                                                                                               | `extensive`     |
  - `none`—No flags are enabled.                                                                                                                   |                 |
  - `accounting`—Route has accounting enabled.                                                                                                   |                 |
  - `cached`—Cache route.                                                                                                                         |                 |
  - `incoming-interface interface-number`—Check against incoming interface.                                                                         |                 |
  - `prefix load balance`—Load balancing is enabled for this prefix.                                                                           |                 |
  - `rt nh decoupled`—Route has been decoupled from the next hop to the destination.                                                             |                 |
  - `sent to PFE`—Route has been sent to the Packet Forwarding Engine.                                                                           |                 |
  - `static`—Static route.                                                                                                                        |                 |
| Next hop            | IP address of the next hop to the destination.                                                                                                                                                                                   | `detail extensive` |

**NOTE:** For static routes that use point-to-point (P2P) outgoing interfaces, the next-hop address is not displayed in the output.
Table 179: show route forwarding-table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next hop Type</td>
<td>Next-hop type. When the <strong>detail</strong> keyword is used, the next-hop type might be</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td>(Type)</td>
<td>abbreviated (as indicated in parentheses):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• broadcast (bcst)—Broadcast.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• deny—Deny.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• discard (dscd)—Discard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hold—Next hop is waiting to be resolved into a unicast or multicast type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• indexed (idxd)—Indexed next hop.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• indirect (indr)—Indirect next hop.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• local (loc)—Local address on an interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• routed multicast (mcrt)—Regular multicast next hop.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast (mcst)—Wire multicast next hop (limited to the LAN).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast discard (mdsc)—Multicast discard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast group (mgrp)—Multicast group member.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• receive (recv)—Receive.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• reject (rjct)—Discard. An ICMP unreachable message was sent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• resolve (rslv)—Resolving the next hop.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unicast (ucst)—Unicast.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unilist (ulst)—List of unicast next hops. A packet sent to this next hop goes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to any next hop in the list.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Software index of the next hop that is used to route the traffic for a given</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>prefix.</td>
<td><strong>none</strong></td>
</tr>
<tr>
<td>Route</td>
<td>Logical interface index from which the route is learned. For example, for interface</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>interface-index</td>
<td>routes, this is the logical interface index of the route itself. For static routes,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>this field is zero. For routes learned through routing protocols, this is the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>logical interface index from which the route is learned.</td>
<td></td>
</tr>
<tr>
<td>Reference (NhRef)</td>
<td>Number of routes that refer to this next hop.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>none</strong></td>
</tr>
<tr>
<td>Next-hop interface</td>
<td>Interface used to reach the next hop.</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td>(Netif)</td>
<td></td>
<td><strong>none</strong></td>
</tr>
<tr>
<td>Weight</td>
<td>Value used to distinguish primary, secondary, and fast reroute backup routes.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>Weight information is available when MPLS label-switched path (LSP) link</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protection, node-link protection, or fast reroute is enabled, or when the standby</td>
<td></td>
</tr>
<tr>
<td></td>
<td>state is enabled for secondary paths. A lower weight value is preferred. Among</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routes with the same weight value, load balancing is possible (see the <strong>Balance</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>field description).</td>
<td></td>
</tr>
<tr>
<td>Balance</td>
<td>Balance coefficient indicating how traffic of unequal cost is distributed among</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>next hops when a router is performing unequal-cost load balancing. This</td>
<td></td>
</tr>
<tr>
<td></td>
<td>information is available when you enable BGP multipath load balancing.</td>
<td></td>
</tr>
<tr>
<td>RPF interface</td>
<td>List of interfaces from which the prefix can be accepted. Reverse path forwarding</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td></td>
<td>(RPF) information is displayed only when <strong>rpf-check</strong> is configured on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Sample Output

#### show route forwarding-table

```
user@host> show route forwarding-table

Routing table: default.inet

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>46</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>dscd</td>
<td>44</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>172.16.1.0/24</td>
<td>iddn</td>
<td>0</td>
<td>172.16.1.0</td>
<td>recv</td>
<td>606</td>
<td>1</td>
<td>1 ge-2/0/1.0</td>
</tr>
<tr>
<td>172.16.1.1/32</td>
<td>user</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>46</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>172.16.1.1/32</td>
<td>intf</td>
<td>0</td>
<td>172.16.1.1</td>
<td>locl</td>
<td>607</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>172.16.1.1/32</td>
<td>iddn</td>
<td>0</td>
<td>172.16.1.1</td>
<td>locl</td>
<td>607</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>172.16.1.255/32</td>
<td>iddn</td>
<td>0</td>
<td>ff:ff:ff:ff:ff:ff</td>
<td>bcst</td>
<td>605</td>
<td>1</td>
<td>1 ge-2/0/1.0</td>
</tr>
<tr>
<td>10.0.0.0/24</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>rslv</td>
<td>616</td>
<td>1</td>
<td>1 ge-2/0/0.0</td>
</tr>
<tr>
<td>10.0.0.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.0.0</td>
<td>locl</td>
<td>615</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.1/32</td>
<td>intf</td>
<td>0</td>
<td>10.0.0.1</td>
<td>locl</td>
<td>615</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.0.255/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.0.255</td>
<td>bcst</td>
<td>613</td>
<td>1</td>
<td>1 ge-2/0/0.0</td>
</tr>
<tr>
<td>10.1.1/24</td>
<td>iddn</td>
<td>0</td>
<td></td>
<td>rslv</td>
<td>612</td>
<td>1</td>
<td>1 ge-2/0/1.0</td>
</tr>
<tr>
<td>10.1.1/32</td>
<td>iddn</td>
<td>0</td>
<td>10.1.1.0</td>
<td>recv</td>
<td>610</td>
<td>1</td>
<td>1 ge-2/0/1.0</td>
</tr>
<tr>
<td>10.1.1/32</td>
<td>user</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>46</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>10.1.1/32</td>
<td>intf</td>
<td>0</td>
<td>10.1.1.1</td>
<td>locl</td>
<td>611</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.1.1/32</td>
<td>iddn</td>
<td>0</td>
<td>10.1.1.1</td>
<td>locl</td>
<td>611</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.1.1/32</td>
<td>iddn</td>
<td>0</td>
<td>ff:ff:ff:ff:ff:ff</td>
<td>bcst</td>
<td>609</td>
<td>1</td>
<td>1 ge-2/0/1.0</td>
</tr>
<tr>
<td>10.206.0.0/16</td>
<td>user</td>
<td>0</td>
<td>10.209.63.254</td>
<td>ucst</td>
<td>419</td>
<td>20</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>10.209.0.0/16</td>
<td>user</td>
<td>1</td>
<td>0:12:1e:ca:98:0</td>
<td>ucst</td>
<td>419</td>
<td>20</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>10.209.0.0/18</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>rslv</td>
<td>418</td>
<td>1</td>
<td>1 fxp0.0</td>
</tr>
<tr>
<td>10.209.0.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.209.0.0</td>
<td>recv</td>
<td>416</td>
<td>1</td>
<td>1 fxp0.0</td>
</tr>
<tr>
<td>10.209.2.131/32</td>
<td>intf</td>
<td>0</td>
<td>10.209.2.131</td>
<td>locl</td>
<td>417</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.209.2.131/32</td>
<td>dest</td>
<td>0</td>
<td>10.209.2.131</td>
<td>locl</td>
<td>417</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.209.17.55/32</td>
<td>dest</td>
<td>0</td>
<td>0:30:48:5b:78:d2</td>
<td>ucst</td>
<td>435</td>
<td>1</td>
<td>1 fxp0.0</td>
</tr>
<tr>
<td>10.209.63.42/32</td>
<td>dest</td>
<td>0</td>
<td>0:23:7d:58:92:ca</td>
<td>ucst</td>
<td>434</td>
<td>1</td>
<td>1 fxp0.0</td>
</tr>
<tr>
<td>10.209.63.254/32</td>
<td>dest</td>
<td>0</td>
<td>0:12:1e:ca:98:0</td>
<td>ucst</td>
<td>419</td>
<td>20</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>10.209.63.255/32</td>
<td>dest</td>
<td>0</td>
<td>10.209.63.255</td>
<td>bcst</td>
<td>415</td>
<td>1</td>
<td>1 fxp0.0</td>
</tr>
<tr>
<td>10.227.0.0/16</td>
<td>user</td>
<td>0</td>
<td>10.209.63.254</td>
<td>ucst</td>
<td>419</td>
<td>20</td>
<td>fxp0.0</td>
</tr>
</tbody>
</table>

...```

#### Routing table: iso

**ISO:**

```
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>27</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>47.0005.80ff.f800.0000.0108.0003.0102.5524.5220.00</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>locl</td>
<td>28</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Routing table: inet6

**Internet6:**

```
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ff00::/8</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>mdsc</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ff02::1/128</td>
<td>perm</td>
<td>0</td>
<td>ff02::1</td>
<td>mcst</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Routing table: ccc

**MPLS:**

```
<table>
<thead>
<tr>
<th>Interface.Label</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
</table>

Copyright © 2019, Juniper Networks, Inc.
show route forwarding-table detail

user@host> show route forwarding-table detail

Routing table: inet

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>user</td>
<td>2</td>
<td>0:90:69:8e:b1:1b</td>
<td>ucst</td>
<td>132</td>
<td>4</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct 16</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>intf</td>
<td>0</td>
<td>ff.3.0.21</td>
<td>ucst</td>
<td>322</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>10.1.1.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.1.1.0</td>
<td>recv</td>
<td>324</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>10.1.1.1/32</td>
<td>intf</td>
<td>0</td>
<td>10.1.1.1</td>
<td>locl</td>
<td>321</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10.1.1.255/32</td>
<td>dest</td>
<td>0</td>
<td>10.1.1.255</td>
<td>bcst</td>
<td>323</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>10.21.21.0/24</td>
<td>intf</td>
<td>0</td>
<td>ff.3.0.21</td>
<td>ucst</td>
<td>326</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>10.21.21.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.21.21.0</td>
<td>recv</td>
<td>328</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>10.21.21.1/32</td>
<td>intf</td>
<td>0</td>
<td>10.21.21.1</td>
<td>locl</td>
<td>325</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10.21.21.255/32</td>
<td>dest</td>
<td>0</td>
<td>10.21.21.255</td>
<td>bcst</td>
<td>327</td>
<td>1</td>
<td>so-5/3/0.0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>intf</td>
<td>0</td>
<td>127.0.0.1</td>
<td>locl</td>
<td>320</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>172.17.28.19/32</td>
<td>clon</td>
<td>1</td>
<td>192.168.4.254</td>
<td>ucst</td>
<td>132</td>
<td>4</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>172.17.28.44/32</td>
<td>clon</td>
<td>1</td>
<td>192.168.4.254</td>
<td>ucst</td>
<td>132</td>
<td>4</td>
<td>fxp0.0</td>
</tr>
</tbody>
</table>

Routing table: private1__.inet

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct 46</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>intf</td>
<td>0</td>
<td>rs1v 136</td>
<td>1</td>
<td>fxp1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.0.0</td>
<td>recv</td>
<td>134</td>
<td>1</td>
<td>fxp1.0</td>
</tr>
<tr>
<td>10.0.0.4/32</td>
<td>intf</td>
<td>0</td>
<td>10.0.0.4</td>
<td>locl</td>
<td>135</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.0.4/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.0.4</td>
<td>locl</td>
<td>135</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Routing table: iso

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct 38</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Routing table: inet6

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct 22</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ff00:/:8</td>
<td>perm</td>
<td>0</td>
<td>mdsc 21</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ff02:/:128</td>
<td>perm</td>
<td>0</td>
<td>mcst 17</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Routing table: mpls

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct 28</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show route forwarding-table destination extensive (Weights and Balances)

user@host> show route forwarding-table destination 3.4.2.1 extensive
### Routing table: inet [Index 0]

**Internet:**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Route type</th>
<th>Route reference</th>
<th>Route interface-index</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4.2.1/32</td>
<td>user</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>sent to PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unilist</td>
<td>Index: 262143</td>
<td>Reference: 1</td>
</tr>
<tr>
<td></td>
<td>172.16.4.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unicast</td>
<td>Index: 335</td>
<td>Reference: 2</td>
</tr>
<tr>
<td></td>
<td>so-1/1/0.0</td>
<td>Weight: 22</td>
<td>Balance: 3</td>
</tr>
<tr>
<td></td>
<td>145.12.1.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unicast</td>
<td>Index: 337</td>
<td>Reference: 2</td>
</tr>
<tr>
<td></td>
<td>so-0/1/2.0</td>
<td>Weight: 33</td>
<td>Balance: 33</td>
</tr>
</tbody>
</table>

---

### show route forwarding-table extensive

```
user@host> show route forwarding-table extensive
Routing table: inet [Index 0]

**Internet:**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Route type</th>
<th>Route reference</th>
<th>Route interface-index</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>user</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>sent to PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unicast</td>
<td>Index: 132</td>
<td>Reference: 4</td>
</tr>
<tr>
<td></td>
<td>fxp0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>permanent</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Index: 14</td>
<td>Reference: 1</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>interface</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>sent to PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>127.0.0.1</td>
<td>Index: 320</td>
<td>Reference: 1</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...  

Routing table: private1__.inet [Index 1]

**Internet:**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Route type</th>
<th>Route reference</th>
<th>Route interface-index</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>permanent</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>sent to PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>reject</td>
<td>Index: 46</td>
<td>Reference: 1</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>interface</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>sent to PFE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>resolve</td>
<td>Index: 136</td>
<td>Reference: 1</td>
</tr>
<tr>
<td></td>
<td>fxp1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Routing table: iso [Index 0]
ISO:

Destination: default
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 38
Reference: 1

Routing table: inet6 [Index 0]
Internet6:

Destination: default
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 22
Reference: 1

Destination: ff00::/8
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: multicast discard
Route interface-index: 0
Index: 21
Reference: 1

Routing table: private1__.inet6 [Index 1]
Internet6:

Destination: default
Route type: permanent
Route reference: 0
Flags: sent to PFE
Next-hop type: reject
Route interface-index: 0
Index: 54
Reference: 1

Destination: fe80::2a0:a5ff:fe3d:375/128
Route type: interface
Route reference: 0
Flags: sent to PFE
Next-hop: fe80::2a0:a5ff:fe3d:375
Next-hop type: local
Route interface-index: 0
Index: 75
Reference: 1

show route forwarding-table extensive (RPF)

The next example is based on the following configuration, which enables an RPF check on all routes that are learned from this interface, including the interface route:

```
so-1/1/0 {
    unit 0 {
        family inet {
            rpf-check;
            address 192.0.2.2/30;
        }
    }
```
user@host> show route forwarding-table extensive
Routing table: inet [Index 0]
Internet: ...
...
Destination: 192.0.2.3/32
  Route type: destination
  Route reference: 0
  Flags: sent to PFE
  Next-hop: 192.0.2.3
  Next-hop type: broadcast
  Index: 328
  Reference: 1
  Next-hop interface: so-1/1/0.0
  RPF interface: so-1/1/0.0

show route forwarding-table extensive (PIM using point-to-multipoint mode)

user@host> show route forwarding-table extensive
Destination: 198.51.100.0/24
  Route type: user
  Route reference: 0
  Multicast RPF nh index: 0
  P2mpidx: 0
  Flags: cached, check incoming interface, accounting, sent to PFE, rt nh decoupled
  Next-hop type: indirect
  Index: 1048575
  Reference: 4
  Nexthop: 
  Next-hop type: composite
  Index: 627
  Reference: 1
  Next-hop type: unicast
  Index: 1048574
  Reference: 2
  Next-hop interface: st0.1, 192.0.2.0

show route forwarding-table (dynamic list next hop)

The show route forwarding table output shows the two next hop elements for a multihomed EVPN destination.

user@host> show route forwarding-table label 299952 extensive
MPLS:

Destination: 299952
  Route type: user
  Route reference: 0
  Multicast RPF nh index: 0
  P2mpidx: 0
  Flags: sent to PFE, rt nh decoupled
  Next-hop type: indirect
  Index: 1048575
  Reference: 2
  Nexthop: 
  Next-hop type: composite
  Index: 601
  Reference: 2
  Next-hop type: indirect
  Index: 1048574
  Reference: 3
  Nexthop: 1.0.0.4
  Next-hop type: Push 301632, Push 299776(top)
  Index: 600
  Reference: 2
  Load Balance Label: None
After one of the PE router has been disabled in the EVPN multihomed network, the same `show route forwarding table` output command shows one next hop element and one empty next hop element.

```
user@host> show route forwarding-table label 299952 extensive
Routing table: default.mpls [Index 0]
MPLS:
Destination: 299952
  Route type: user
  Route reference: 0
  Route interface-index: 0
  Multicast RPF nh index: 0
  P2mpidx: 0
  Flags: sent to PFE, rt nh decoupled
  Next-hop type: indirect
  Index: 1048575
  Reference: 2
  Nexthop: 1.0.0.4
  Next-hop type: composite
  Index: 601
  Reference: 2
  Load Balance Label: None
  Next-hop interface: ge-0/0/1.0
```

```
show route forwarding-table family mpls
user@host> show route forwarding-table family mpls
Routing table: mpls
MPLS:
Destination        Type RtRef Next hop          Type Index NhRef Netif
default            perm     0                   rjct    19     1
0                  user     0                   recv    18     3
1                  user     0                   recv    18     3
2                  user     0                   recv    18     3
100000             user     0 10.31.1.6         swap  100001     fe-1/1/0.0
800002             user     0                   indr   351     4
vt-0/3/0.32770 (VPLS)
                      user     0                   indr   351     4
so-0/0/0.0
```

```
show route forwarding-table family mpls ccc ge-0/0/1.1004
user@host>show route forwarding-table mpls ccc ge-0/0/1.1004
Routing table: default.mpls
MPLS:
Destination        Type RtRef Next hop          Type Index NhRef Netif
ge-0/0/1.1004 (CCC) user     0                   ulst  1048577     2
```

show route forwarding-table family vpls

user@host> show route forwarding-table family vpls

Routing table: green.vpls
VPLS:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>dscd</td>
<td>556</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>rjct</td>
<td>298</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>fe-0/1/0.0</td>
<td>dynm</td>
<td>0</td>
<td></td>
<td>flood</td>
<td>355</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>00:00:5E:00:53:1f/48</td>
<td>dynm</td>
<td>0</td>
<td></td>
<td>indr</td>
<td>351</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>dynm</td>
<td>0</td>
<td></td>
<td>flood</td>
<td>355</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>00:00:5E:00:53:1f/48</td>
<td>dynm</td>
<td>0</td>
<td></td>
<td>indr</td>
<td>351</td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

Remote CE

Local CE

show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled)

user@host> show route forwarding-table vpls

Routing table: green.vpls
VPLS:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>dscd</td>
<td>519</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>lsi.1048832</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>indr</td>
<td>1048574</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>172.16.3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Push 262145</td>
<td>621</td>
<td>2</td>
</tr>
<tr>
<td>ge-3/0/0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Push 262145</td>
<td>621</td>
<td>2</td>
</tr>
<tr>
<td>00:00:5E:00:53:01/48</td>
<td>user</td>
<td>0</td>
<td></td>
<td>ucst</td>
<td>590</td>
<td>5</td>
<td>ge-2/3/9.0</td>
</tr>
<tr>
<td>0x30003/51</td>
<td>user</td>
<td>0</td>
<td></td>
<td>comp</td>
<td>627</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ge-2/3/9.0</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>ucst</td>
<td>590</td>
<td>5</td>
<td>ge-2/3/9.0</td>
</tr>
<tr>
<td>ge-3/1/3.0</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>ucst</td>
<td>619</td>
<td>4</td>
<td>ge-3/1/3.0</td>
</tr>
<tr>
<td>0x30002/51</td>
<td>user</td>
<td>0</td>
<td></td>
<td>comp</td>
<td>600</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>0x30001/51</td>
<td>user</td>
<td>0</td>
<td></td>
<td>comp</td>
<td>597</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

show route forwarding-table vpls (Broadcast, unknown unicast, and multicast (BUM) hashing is enabled with MAC Statistics)

user@host> show route forwarding-table vpls

Routing table: green.vpls
VPLS:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td></td>
<td>dscd</td>
<td>519</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>lsi.1048834</td>
<td>intf</td>
<td>0</td>
<td></td>
<td>indr</td>
<td>1048574</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>172.16.3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Push 262145</td>
<td>592</td>
<td>2</td>
</tr>
</tbody>
</table>
show route forwarding-table family vpls extensive

user@host> show route forwarding-table family vpls extensive

Routing table: green.vpls [Index 2]
VPLS:

Destination: default
Route type: dynamic
Route reference: 0
Flags: sent to PFE
Next-hop type: flood
Index: 289 Reference: 1
Next-hop type: unicast
Index: 291 Reference: 3
Next-hop interface: fe-0/1/3.0
Next-hop type: unicast
Index: 290 Reference: 3
Next-hop interface: fe-0/1/2.0

Destination: default
Route type: permanent
Route reference: 0
Flags: none
Next-hop type: discard
Index: 341 Reference: 1

Destination: fe-0/1/2.0
Route type: dynamic
Route reference: 0
Flags: sent to PFE
Next-hop type: flood
Index: 293 Reference: 1
Next-hop type: indirect
Index: 363 Reference: 4
Next-hop type: Push 800016
Next-hop interface: at-1/0/1.0
Next-hop type: indirect
Index: 301 Reference: 5
Next hop: 10.31.3.2
Next-hop type: Push 800000
Next-hop interface: fe-0/1/1.0
Next-hop type: unicast
Next-hop interface: fe-0/1/3.0

Destination: fe-0/1/3.0
Route type: dynamic
Route reference: 0
Flags: sent to PFE
Next-hop type: flood
Index: 292 Reference: 1
Next-hop type: indirect
Index: 363 Reference: 4
Next-hop type: Push 800016
Next-hop interface: at-1/0/1.0
Next-hop type: indirect
Index: 301 Reference: 5
Next hop: 10.31.3.2
Next-hop type: Push 800000
Next-hop interface: fe-0/1/1.0
Next-hop type: unicast
Next-hop interface: fe-0/1/2.0
### show route forwarding-table table default

```
user@host> show route forwarding-table table default
Routting table: default.inet
Internet:
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>36</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>perm</td>
<td>0</td>
<td>dscd</td>
<td>34</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.60.0/30</td>
<td>user</td>
<td>0</td>
<td>10.0.60.13</td>
<td>ucst</td>
<td>713</td>
<td>5</td>
<td>fe-0/1/3.0</td>
</tr>
<tr>
<td>10.0.60.12/30</td>
<td>intf</td>
<td>0</td>
<td>rslv</td>
<td>688</td>
<td>1</td>
<td>fe-0/1/3.0</td>
<td></td>
</tr>
<tr>
<td>10.0.60.12/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.60.12</td>
<td>recv</td>
<td>686</td>
<td>1</td>
<td>fe-0/1/3.0</td>
</tr>
<tr>
<td>10.0.60.13/32</td>
<td>dest</td>
<td>0</td>
<td>0:5:85:8b:bc:22</td>
<td>ucst</td>
<td>713</td>
<td>5</td>
<td>fe-0/1/3.0</td>
</tr>
<tr>
<td>10.0.60.14/32</td>
<td>intf</td>
<td>0</td>
<td>locl</td>
<td>687</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.60.14/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.60.14</td>
<td>locl</td>
<td>687</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.60.15/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.60.15</td>
<td>bcst</td>
<td>685</td>
<td>1</td>
<td>fe-0/1/3.0</td>
</tr>
<tr>
<td>10.0.67.12/30</td>
<td>user</td>
<td>0</td>
<td>10.0.60.13</td>
<td>ucst</td>
<td>713</td>
<td>5</td>
<td>fe-0/1/3.0</td>
</tr>
<tr>
<td>10.0.80.0/30</td>
<td>ifdn</td>
<td>0</td>
<td>ff.3.0.21</td>
<td>ucst</td>
<td>676</td>
<td>1</td>
<td>so-0/0/1.0</td>
</tr>
<tr>
<td>10.0.80.0/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.80.0</td>
<td>recv</td>
<td>678</td>
<td>1</td>
<td>so-0/0/1.0</td>
</tr>
<tr>
<td>10.0.80.2/32</td>
<td>user</td>
<td>0</td>
<td>rjct</td>
<td>36</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.0.80.2/32</td>
<td>intf</td>
<td>0</td>
<td>10.0.80.2</td>
<td>locl</td>
<td>675</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10.0.80.3/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.80.3</td>
<td>bcst</td>
<td>677</td>
<td>1</td>
<td>so-0/0/1.0</td>
</tr>
<tr>
<td>10.0.90.12/30</td>
<td>intf</td>
<td>0</td>
<td>rslv</td>
<td>684</td>
<td>1</td>
<td>fe-0/1/0.0</td>
<td></td>
</tr>
<tr>
<td>10.0.90.12/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.90.12</td>
<td>recv</td>
<td>682</td>
<td>1</td>
<td>fe-0/1/0.0</td>
</tr>
<tr>
<td>10.0.90.14/32</td>
<td>intf</td>
<td>0</td>
<td>10.0.90.14</td>
<td>locl</td>
<td>683</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.90.14/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.90.14</td>
<td>locl</td>
<td>683</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>10.0.90.15/32</td>
<td>dest</td>
<td>0</td>
<td>10.0.90.15</td>
<td>bcst</td>
<td>681</td>
<td>1</td>
<td>fe-0/1/0.0</td>
</tr>
<tr>
<td>10.5.0.0/16</td>
<td>user</td>
<td>0</td>
<td>192.168.187.126</td>
<td>ucst</td>
<td>324</td>
<td>15</td>
<td>fxp0.0</td>
</tr>
</tbody>
</table>
```
### show route forwarding-table table logical-system-name/routing-instance-name

```bash
user@host> show route forwarding-table table R4/vpn-red

*** Logical system: R4 ***
Routing table: vpn-red.inet
Internet:
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type Ref</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>563</td>
<td>1</td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>perm</td>
<td>0</td>
<td>dscd</td>
<td>561</td>
<td>2</td>
</tr>
<tr>
<td>172.16.0.1/32</td>
<td>user</td>
<td>0</td>
<td>dscd</td>
<td>561</td>
<td>2</td>
</tr>
<tr>
<td>172.16.2.0/24</td>
<td>intf</td>
<td>0</td>
<td>rslv</td>
<td>771</td>
<td>1 ge-1/2/0.3</td>
</tr>
<tr>
<td>172.16.2.0/32</td>
<td>dest</td>
<td>0 172.16.2.0</td>
<td>recv</td>
<td>769</td>
<td>1 ge-1/2/0.3</td>
</tr>
<tr>
<td>172.16.2.1/32</td>
<td>intf</td>
<td>0 172.16.2.1</td>
<td>locl</td>
<td>770</td>
<td>2</td>
</tr>
<tr>
<td>172.16.2.2/32</td>
<td>dest</td>
<td>0 0.4.80.3.0.1b.c0.d5.e4.bd.0.1b.c0.d5.e4.bc.8.0</td>
<td>locl</td>
<td>770</td>
<td>2</td>
</tr>
<tr>
<td>172.16.2.255/32</td>
<td>dest</td>
<td>0 172.16.2.255</td>
<td>bcst</td>
<td>768</td>
<td>1 ge-1/2/0.3</td>
</tr>
<tr>
<td>172.16.233.0/4</td>
<td>perm</td>
<td>1</td>
<td>mdsc</td>
<td>562</td>
<td>1</td>
</tr>
<tr>
<td>172.16.233.1/32</td>
<td>perm</td>
<td>0 172.16.233.1</td>
<td>mcsd</td>
<td>558</td>
<td>1</td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>perm</td>
<td>0</td>
<td>bcst</td>
<td>559</td>
<td>1</td>
</tr>
</tbody>
</table>

*** Logical system: R4 ***
Routing table: vpn-red.iso
ISO:
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type Ref</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>608</td>
<td>1</td>
</tr>
</tbody>
</table>

*** Logical system: R4 ***
Routing table: vpn-red.inet6
Internet6:
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type Ref</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>708</td>
<td>1</td>
</tr>
</tbody>
</table>
```
show route forwarding-table vpn

user@host> show route forwarding-table vpn VPN-A

Routing table:: VPN-A.inet
Internet:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type RfRef</th>
<th>Nexthop</th>
<th>Type Index NhRef Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>dscd 638</td>
</tr>
<tr>
<td>10.39.10.20/30</td>
<td>intf</td>
<td>0</td>
<td>ucst 40 1</td>
</tr>
<tr>
<td>10.39.10.21/32</td>
<td>intf</td>
<td>0 10.39.10.21</td>
<td>locl 36 1</td>
</tr>
<tr>
<td>10.255.14.172/32</td>
<td>user</td>
<td>0</td>
<td>ucst 69 2</td>
</tr>
<tr>
<td>10.255.14.175/32</td>
<td>user</td>
<td>0</td>
<td>indr 81 3</td>
</tr>
<tr>
<td>100004(top) so-1/0/0.0</td>
<td>user</td>
<td>0 100004</td>
<td>Push 100004, Push</td>
</tr>
<tr>
<td>172.16.233.0/4</td>
<td>perm</td>
<td>2 172.16.233.1</td>
<td>mcst 1 8</td>
</tr>
<tr>
<td>172.16.233.5/32</td>
<td>user</td>
<td>1 172.16.233.5</td>
<td>mcst 1 8</td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>perm</td>
<td>0</td>
<td>bcst 2 3</td>
</tr>
</tbody>
</table>

On QFX5200, the results for this command look like this:

show route forwarding-table family mpls

Routing table: default.mpls
MPLS:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type RfRef</th>
<th>Nexthop</th>
<th>Type Index NhRef Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>dscd 706 1</td>
</tr>
<tr>
<td>ff00::/8</td>
<td>perm</td>
<td>0</td>
<td>mdsc 707 1</td>
</tr>
<tr>
<td>ff02::1/128</td>
<td>perm</td>
<td>0 ff02::1</td>
<td>mcst 704 1</td>
</tr>
</tbody>
</table>

Routing table: __mpls-oam__.mpls
MPLS:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type RfRef</th>
<th>Nexthop</th>
<th>Type Index NhRef Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>dscd 65 1</td>
</tr>
<tr>
<td>0</td>
<td>user</td>
<td>0</td>
<td>recv 64 4</td>
</tr>
<tr>
<td>1</td>
<td>user</td>
<td>0</td>
<td>recv 64 4</td>
</tr>
<tr>
<td>13</td>
<td>user</td>
<td>0</td>
<td>recv 64 4</td>
</tr>
<tr>
<td>300384 user 0 9.1.1.1 Pop 1711 2 xe-0/0/34.0</td>
<td>user 0 9.1.1.1 Pop 1712 2 xe-0/0/34.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>300400 user 0 ulst 131071 2</td>
<td>user 0 131071 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.1.2 Pop 1713 1 xe-0/0/38.0 172.16.11.2 Pop 1714 1 xe-0/0/40.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>300400 user 0 ulst 131072 2</td>
<td>user 0 131072 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.1.2 Pop 1715 1 xe-0/0/38.0 172.16.11.2 Pop 1716 1 xe-0/0/40.0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show route forwarding-table interface-name

Syntax

show route forwarding-table interface-name interface-name
<detail | extensive>
<all>

Release Information

Description
Display the interfaces in the Routing Engine’s forwarding table.

Options
none—Display information for the specified interface.
detail | extensive—(Optional) Display the specified level of output.
all—(Optional) Display all interfaces in the routing table.

Required Privilege
view

List of Sample Output
show route forwarding-table interface-name fe-0/1/1 on page 2373
show route forwarding-table interface-name all on page 2373
show route forwarding-table interface-name all detail on page 2374

Output Fields
Table 180 on page 2372 lists the output fields for the show route forwarding-table interface-name command. Output fields are listed in the approximate order in which they appear.

Table 180: show route forwarding-table interface-name Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the interface (for example fe-0/1/1, lo0, ae0, and so on).</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Interface’s maximum transmission unit (MTU).</td>
<td>All levels</td>
</tr>
<tr>
<td>Afam</td>
<td>Configured address family (for example inet, tnp, inet6, and so on).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Network</td>
<td>Network information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• &lt;Link&gt;—Physical interface, not a logical interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;PtoP&gt;—Point-to-point network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ipaddress—Network address.</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Address of the interface. The address can be a MAC address, IPv4 address, IPv6 address, and so on.</td>
<td>All levels</td>
</tr>
<tr>
<td>IPkts</td>
<td>Number of packets received on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Ierr</td>
<td>Number of packets received on the interface with errors.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 180: show route forwarding-table interface-name Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opkts</td>
<td>Number of packets transmitted or sent from the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Oerr</td>
<td>Number of packets transmitted or sent from the interface with errors.</td>
<td>All levels</td>
</tr>
<tr>
<td>Coll</td>
<td>Number of packets that experienced collisions on the interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show route forwarding-table interface-name fe-0/1/1

```
user@host> show route forwarding-table interface-name fe-0/1/1

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>Network</th>
<th>Address</th>
<th>Ipkts</th>
<th>Ierr</th>
<th>Opkts</th>
<th>Oerr</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/1/1</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

show route forwarding-table interface-name all

```
user@host> show route forwarding-table interface-name all

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>Network</th>
<th>Address</th>
<th>Ipkts</th>
<th>Ierr</th>
<th>Opkts</th>
<th>Oerr</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>fxp0</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.a0.a5.03.83</td>
<td>180965</td>
<td>0</td>
<td>39907</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 0</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>02.00.00.00.00.04</td>
<td>33010497</td>
<td>0</td>
<td>30110800</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fxp1</td>
<td>1500</td>
<td>192.168.187.0/24</td>
<td>192.168.187.10</td>
<td>33010497</td>
<td>0</td>
<td>30110800</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 0</td>
<td>1500</td>
<td>192.168.187.0/24</td>
<td>192.168.187.10</td>
<td>33010497</td>
<td>0</td>
<td>30110800</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lsi</td>
<td>1496</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dsc</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lo0</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 0</td>
<td>max</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>0</td>
<td>127.0.0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 16384</td>
<td>max</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>0</td>
<td>127.0.0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 16385</td>
<td>max</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>0</td>
<td>127.0.0.1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>gre</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ipip</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tap</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pime</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>pimd</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mtun</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 0</td>
<td>max</td>
<td>10.0.60.2/32</td>
<td>10.0.60.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>so-0/0/1</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unit 0</td>
<td>max</td>
<td>10.0.80.2/32</td>
<td>10.0.80.2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show route forwarding-table interface-name all detail

```
user@host> show route forwarding-table interface-name all detail

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>AFam</th>
<th>Network</th>
<th>Address</th>
<th>Ipkts</th>
<th>Ierr</th>
<th>Opkts</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpx0</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.a0.a5.56.03.83</td>
<td>181005</td>
<td>0</td>
<td>39948</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unit 0</td>
<td>1500</td>
<td>inet</td>
<td>192.168.187.0/192.168.187.10</td>
<td>02.00.00.00.04</td>
<td>33012676</td>
<td>0</td>
<td>3012468</td>
<td></td>
</tr>
<tr>
<td>fpx1</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>02.00.00.00.04</td>
<td>33012676</td>
<td>0</td>
<td>39948</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unit 0</td>
<td>1500</td>
<td>inet</td>
<td>192.168.187.0/192.168.187.10</td>
<td>02.00.00.00.04</td>
<td>33012676</td>
<td>0</td>
<td>3012468</td>
<td></td>
</tr>
<tr>
<td>lsi</td>
<td>1496</td>
<td>&lt;Link&gt;</td>
<td>00.a0.a5.56.03.83</td>
<td>181005</td>
<td>0</td>
<td>39948</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dsc</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>02.00.00.00.04</td>
<td>33012676</td>
<td>0</td>
<td>39948</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lo0</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unit 0</td>
<td>max</td>
<td>inet</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unit 16384</td>
<td>max</td>
<td>inet</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>unit 16385</td>
<td>max</td>
<td>inet</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gre</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipip</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tap</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pime</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pimd</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mtun</td>
<td>max</td>
<td>&lt;Link&gt;</td>
<td>127.0.0.1/8</td>
<td>127.0.0.1</td>
<td>0</td>
<td>8980</td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>4474</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.88.cc.1f</td>
<td>523120</td>
<td>623044</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>so-0/0/3</td>
<td>4474</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.88.cc.1f</td>
<td>523120</td>
<td>623044</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>fe-0/1/0</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.88.cc.20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>fe-0/1/1</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.88.cc.21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>fe-0/1/2</td>
<td>1514</td>
<td>&lt;Link&gt;</td>
<td>00.05.85.88.cc.21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

show route hidden

Syntax
show route hidden
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Display only hidden route information. A hidden route is unusable, even if it is the best path.

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.

Required Privilege
view

Related Documentation
• Understanding Hidden Routes

List of Sample Output
show route hidden on page 2375
show route hidden detail on page 2376
show route hidden extensive on page 2376
show route hidden terse on page 2377

Output Fields
For information about output fields, see the output field table 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 hidden

user@host> show route hidden
inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
   Restart Complete
+ = Active Route, - = Last Active, * = Both
  127.0.0.1/32        [Direct/0] 04:26:38
       > via lo0.0
private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
   Restart Complete
+ = Active Route, - = Last Active, * = Both
<table>
<thead>
<tr>
<th>Route</th>
<th>Source Information</th>
</tr>
</thead>
</table>
| 10.5.5.5/32      | [BGP/170] 03:44:10, localpref 100, from 10.4.4.4  
|                  | AS path: 100 I                              |
|                  | Unusable                                     |
| 10.12.1.0/24     | [BGP/170] 03:44:10, localpref 100, from 10.4.4.4  
|                  | AS path: 100 I                              |
|                  | Unusable                                     |
| 10.12.80.4/30    | [BGP/170] 03:44:10, localpref 100, from 10.4.4.4  
|                  | AS path: I                                  |
|                  | Unusable                                     |
| ...              |                                              |

**show route hidden detail**

```shell
user@host> show route hidden detail

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)  
Restart Complete
127.0.0.1/32 (1 entry, 0 announced)
   Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 1
   Next hop: via lo0.0, selected
   State: <Hidden Martian Int>
   Local AS:     1
   Age: 4:27:37
   Task: IF
   AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)  
Restart Complete
10.5.5.5/32 (1 entry, 0 announced)
   BGP   Preference: 170/-101
   Route Distinguisher: 10.4.4.4:4
   Next hop type: Unusable
   Next-hop reference count: 6
   State: <Secondary Hidden Int Ext>
   Local AS:     1 Peer AS:     1
   Age: 3:45:09
   Task: BGP_1.10.4.4.4+2493
   AS path: 100 I
   Communities: target:1:999
   VPN Label: 100064
   Localpref: 100
   Router ID: 10.4.4.4
   Primary Routing Table bgp.l3vpn.0

...```

**show route hidden extensive**

The output for the `show route hidden extensive` command is identical to that of the `show route hidden detail` command. For sample output, see `show route hidden detail` on page 2376.
show route hidden terse

```
user@host> show route hidden terse

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A 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>127.0.0.1/32</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
</tbody>
</table>

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A 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>10.5.5.5/32</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>100 I</td>
</tr>
<tr>
<td>10.12.1.0/24</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>100 I</td>
</tr>
<tr>
<td>10.12.80.4/30</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>I</td>
</tr>
</tbody>
</table>

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

bgp.l3vpn.0: 3 destinations, 3 routes (0 active, 0 holddown, 3 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A 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>10.4.4.4:4:10.5.5.5/32</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>100 I</td>
</tr>
<tr>
<td>10.4.4.4:4:10.12.1.0/24</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>100 I</td>
</tr>
<tr>
<td>10.4.4.4:4:10.12.80.4/30</td>
<td>B</td>
<td>170</td>
<td>100</td>
<td></td>
<td>Unusable</td>
<td>I</td>
</tr>
</tbody>
</table>

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```
show route inactive-path

List of Syntax  Syntax on page 2378
Syntax (EX Series Switches) on page 2378

Syntax  show route inactive-path
        <brief | detail | extensive | terse>
        <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route inactive-path
        <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.

Description  Display routes for destinations that have no active route. An inactive route is a route that
was not selected as the best path.

Options  none—Display all inactive routes.
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.

Required Privilege  view

Related Documentation  • show route active-path on page 2273

List of Sample Output  show route inactive-path on page 2378
show route inactive-path detail on page 2379
show route inactive-path extensive on page 2380
show route inactive-path terse on page 2380

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 inactive-path

    user@host> show route inactive-path
inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.12.100.12/30  [OSPF/10] 03:57:28, metric 1
    > via so-0/3/0.0

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.0/8         [Direct/0] 04:39:56
    > via fxp1.0

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.12.80.0/30      [BGP/170] 04:38:17, localpref 100
    AS path: 100 I
    > to 10.12.80.1 via ge-6/3/2.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

bgp.l3vpn.0: 3 destinations, 3 routes (0 active, 0 holddown, 3 hidden)
Restart Complete

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

show route inactive-path detail

user@host> show route inactive-path detail

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete

10.12.100.12/30 (2 entries, 1 announced)
    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:  1
    Age: 3:58:24  Metric: 1
    Area: 0.0.0.0
    Task: OSPF
    AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

10.0.0.0/8 (2 entries, 0 announced)
    Direct Preference: 0
show route inactive-path extensive

The output for the `show route inactive-path extensive` command is identical to that of the `show route inactive-path detail` command. For sample output, see `show route inactive-path detail on page 2379`.

show route inactive-path terse

```
user@host> show route inactive-path terse

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
10.12.100.12/30    O  10          1            >so-0/3/0.0

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
10.0.0.0/8         D   0                       >fxp1.0

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
10.12.80.0/30      B 170        100            >10.12.80.1      100 I
```
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

bgp.l3vpn.0: 3 destinations, 3 routes (0 active, 0 holddown, 3 hidden)
Restart Complete

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
show route inactive-prefix

List of Syntax  
Syntax on page 2382  
Syntax (EX Series Switches) on page 2382

Syntax  
show route inactive-prefix  
<brief | detail | extensive | terse>  
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  
show route inactive-prefix  
<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.

Description  
Display inactive route destinations in each routing table.

Options  
none—Display all inactive route destination.  
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.

Required Privilege  
view

List of Sample Output  
show route inactive-prefix on page 2382  
show route inactive-prefix detail on page 2383  
show route inactive-prefix extensive on page 2383  
show route inactive-prefix terse on page 2383

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 inactive-prefix

user@host> show route inactive-prefix

inet.0: 14 destinations, 14 routes (13 active, 0 holddown, 1 hidden)  
+ = Active Route, - = Last Active, * = Both
show route inactive-prefix detail

user@host> show route inactive-prefix detail

inet.0: 14 destinations, 14 routes (13 active, 0 holddown, 1 hidden)
127.0.0.1/32 (1 entry, 0 announced)
  Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Hidden Martian Int>
  Age: 4:51
  Task: IF
  AS path: 100:04:54
    > via lo0.0

show route inactive-prefix extensive

The output for the `show route inactive-prefix extensive` command is identical to that of the `show route inactive-path detail` command. For sample output, see `show route inactive-prefix detail on page 2383`.

show route inactive-prefix terse

user@host> show route inactive-prefix terse

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination P Prf Metric 1 Metric 2 Next hop AS path
127.0.0.1/32  D  0        >lo0.0
show route instance

List of Syntax

Syntax

show route instance
<brief | detail | summary>
<instance-name>
<logical-system (all | logical-system-name)>
<operational>

Syntax (EX Series Switches and QFX Series)

show route instance
<brief | detail | summary>
<instance-name>
<logical-system (all | logical-system-name)>
<operational>

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 11.3 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

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 all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the show route instance cust1 command).

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

operational—(Optional) Display operational routing instances.

Required Privilege Level

view

Related Documentation

• Example: Transporting IPv6 Traffic Across IPv4 Using Filter-Based Tunneling
• Example: Configuring the Helper Capability Mode for OSPFv3 Graceful Restart

List of Sample Output

show route instance on page 2384
show route instance detail (Graceful Restart Complete) on page 2386
show route instance detail (Graceful Restart Incomplete) on page 2388
show route instance detail (VPLS Routing Instance) on page 2390
show route instance operational on page 2390
show route instance summary on page 2390

**Output Fields**

Table 181 on page 2385 lists the output fields for the `show route instance` command. Output fields are listed in the approximate order in which they appear.

**Table 181: 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>
<tr>
<td>Operational Routing Instances</td>
<td>(operational keyword only) Names of all operational routing instances.</td>
<td>—</td>
</tr>
<tr>
<td>Type</td>
<td>Type of routing instance: forwarding, l2vpn, no-forwarding, vpls, virtual-router, or vrf.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the routing instance: active or inactive.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Name of interfaces belonging to this routing instance.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Restart State</td>
<td>Status of graceful restart for this instance: Pending or Complete.</td>
<td>detail</td>
</tr>
<tr>
<td>Path selection timeout</td>
<td>Maximum amount of time, in seconds, remaining until graceful restart is declared complete. The default is 300.</td>
<td>detail</td>
</tr>
<tr>
<td>Tables</td>
<td>Tables (and number of routes) associated with this routing instance.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Route-distinguisher</td>
<td>Unique route distinguisher associated with this routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-import</td>
<td>VPN routing and forwarding instance import policy name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-export</td>
<td>VPN routing and forwarding instance export policy name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-import-target</td>
<td>VPN routing and forwarding instance import target community name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-export-target</td>
<td>VPN routing and forwarding instance export target community name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-edge-protection-id</td>
<td>Context identifier configured for edge-protection.</td>
<td>detail</td>
</tr>
<tr>
<td>Fast-reroute-priority</td>
<td>Fast reroute priority setting for a VPLS routing instance: high, medium, or low. The default is low.</td>
<td>detail</td>
</tr>
<tr>
<td>Restart State</td>
<td>Restart state:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Pending:protocol-name—List of protocols that have not yet completed graceful restart for this routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Complete—All protocols have restarted for this routing table.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 181: 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>Primary rib</td>
<td>Primary table for this routing instance.</td>
<td>brief none summary</td>
</tr>
<tr>
<td>Active/holddown/hidden</td>
<td>Number of active, hold-down, and hidden routes.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

### Sample Output

**show route instance**

```
user@host> show route instance
```

```
+-----------------+--------------+--------------------------+
| Instance        | Primary RIB  | Active/holddown/hidden   |
| master          | forwarding   |                          |
| inet.0          |              | 16/0/1                   |
| iso.0           |              | 1/0/0                    |
| mpls.0          |              | 0/0/0                    |
| inet6.0         |              | 2/0/0                    |
| l2circuit.0     |              | 0/0/0                    |
| __juniper_private1__.inet.0 | | 12/0/0 |
| __juniper_private1__.inet6.0 | | 1/0/0 |
```

**show route instance detail (Graceful Restart Complete)**

```
user@host> show route instance detail
```

```
master:
  Router ID: 10.255.14.176
  Type: forwarding State: Active
  Restart State: Complete Path selection timeout: 300
  Tables:
  inet.0 : 17 routes (15 active, 0 holddown, 1 hidden)
  inet.3 : 2 routes (2 active, 0 holddown, 0 hidden)
  iso.0  : 1 routes (1 active, 0 holddown, 0 hidden)
  mpls.0 : 19 routes (19 active, 0 holddown, 0 hidden)
  bgp.l3vpn.0 : 10 routes (10 active, 0 holddown, 0 hidden)
  bgp.l2vpn.0 : 1 routes (1 active, 0 holddown, 0 hidden)
  bgp.l2vpn.1 : 1 routes (1 active, 0 holddown, 0 hidden)

BGP-INET:
  Router ID: 10.69.103.1
  Type: vrf State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.103
  Route-distinguisher: 10.255.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
```
Tables:
  BGP-INET.inet.0        : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
BGP-L:
  Router ID: 10.69.104.1
  Type: vrf           State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.104
  Route-distinguisher: 10.255.14.176:104
  Vrf-import: [BGP-L-import]
  Vrf-export: [BGP-L-export]
  Tables:
  BGP-L.inet.0        : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
  BGP-L.mpls.0        : 3 routes (3 active, 0 holddown, 0 hidden)
  Restart Complete
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn         State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.512
  Route-distinguisher: 10.255.14.176:512
  Vrf-import: [L2VPN-import]
  Vrf-export: [L2VPN-export]
  Tables:
  L2VPN.l2vpn.0      : 2 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete
LDP:
  Router ID: 10.69.105.1
  Type: vrf           State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.105
  Route-distinguisher: 10.255.14.176:105
  Vrf-import: [LDP-import]
  Vrf-export: [LDP-export]
  Tables:
  LDP.inet.0         : 5 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
OSPF:
  Router ID: 10.69.101.1
  Type: vrf           State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.101
  Vrf-import: [OSPF-import]
  Vrf-export: [OSPF-export]
  Vrf-import-target: [target:11111]
  Tables:
  OSPF.inet.0        : 8 routes (7 active, 0 holddown, 0 hidden)
  Restart Complete
RIP:
  Router ID: 10.69.102.1
  Type: vrf           State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
  t3-0/0/0.102
Vrf-import: [ RIP-import ]
Vrf-export: [ RIP-export ]

Tables:
- RIP.inet.0 : 6 routes (6 active, 0 holddown, 0 hidden)
- Restart Complete

**STATIC:**
Router ID: 10.69.100.1
Type: vrf State: Active
Restart State: Complete Path selection timeout: 300

Interfaces:
- t3-0/0/0.100
Route-distinguisher: 10.255.14.176:100
Vrf-import: [ STATIC-import ]
Vrf-export: [ STATIC-export ]

Tables:
- STATIC.inet.0 : 4 routes (4 active, 0 holddown, 0 hidden)
- Restart Complete

---

**show route instance detail (Graceful Restart Incomplete)**

```
user@host> show route instance detail

master:
- Router ID: 10.255.14.176
- Type: forwarding State: Active
- Restart State: Pending Path selection timeout: 300
- Tables:
  - inet.0 : 17 routes (15 active, 1 holddown, 1 hidden)
  - Restart Pending: OSPF LDP
  - inet.3 : 2 routes (2 active, 0 holddown, 0 hidden)
  - Restart Pending: OSPF LDP
  - iso.0 : 1 routes (1 active, 0 holddown, 0 hidden)
  - Restart Complete
  - mpls.0 : 23 routes (23 active, 0 holddown, 0 hidden)
  - Restart Pending: LDP VPN
  - bgp.13vpn.0 : 10 routes (10 active, 0 holddown, 0 hidden)
  - Restart Pending: BGP VPN
  - inet6.0 : 2 routes (2 active, 0 holddown, 0 hidden)
  - Restart Complete
  - bgp.12vpn.0 : 1 routes (1 active, 0 holddown, 0 hidden)
  - Restart Pending: BGP VPN

BGP-INET:
- Router ID: 10.69.103.1
- Type: vrf State: Active
- Restart State: Pending Path selection timeout: 300
- Interfaces:
  - t3-0/0/0.103
- Route-distinguisher: 10.255.14.176:103
- Vrf-import: [ BGP-INET-import ]
- Vrf-export: [ BGP-INET-export ]
- Tables:
  - BGP-INET.inet.0 : 6 routes (5 active, 0 holddown, 0 hidden)
  - Restart Pending: VPN

BGP-L:
- Router ID: 10.69.104.1
- Type: vrf State: Active
- Restart State: Pending Path selection timeout: 300
- Interfaces:
  - t3-0/0/0.104
```
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Router ID</th>
<th>Type</th>
<th>State</th>
<th>Restart State</th>
<th>Path selection timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP-L</td>
<td>10.69.101.1</td>
<td>vrf</td>
<td>Active</td>
<td>Pending</td>
<td>300</td>
</tr>
<tr>
<td>L2VPN</td>
<td>10.69.101.1</td>
<td>vrf</td>
<td>Active</td>
<td>Pending</td>
<td>300</td>
</tr>
<tr>
<td>OSPF</td>
<td>10.69.102.1</td>
<td>vrf</td>
<td>Active</td>
<td>Pending</td>
<td>300</td>
</tr>
<tr>
<td>RIP</td>
<td>10.69.102.1</td>
<td>vrf</td>
<td>Active</td>
<td>Pending</td>
<td>300</td>
</tr>
<tr>
<td>STATIC</td>
<td>10.69.100.1</td>
<td>vrf</td>
<td>Active</td>
<td>Pending</td>
<td>300</td>
</tr>
</tbody>
</table>
Interfaces:
  t3-0/0/0.100
  Route-distinguisher: 10.255.14.176:100
  Vrf-import: [ STATIC-import ]
  Vrf-export: [ STATIC-export ]
Tables:
  STATIC.inet.0 : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Pending: VPN

show route instance detail (VPLS Routing Instance)

user@host> show route instance detail test-vpls

  test-vpls:
    Router ID: 0.0.0.0
    Type: vpls              State: Active
    Interfaces:
      lsi.1048833
      lsi.1048832
      fe-0/1/0.513
    Route-distinguisher: 10.255.37.65:1
    Vrf-import: [ __vrf-import-test-vpls-internal__ ]
    Vrf-export: [ __vrf-export-test-vpls-internal__ ]
    Vrf-import-target: [ target:300:1 ]
    Vrf-export-target: [ target:300:1 ]
    Vrf-edge-protection-id: 166.1.3.1  Fast-reroute-priority: high
Tables:
  test-vpls.l2vpn.0 : 3 routes (3 active, 0 holddown, 0 hidden)

show route instance operational

user@host> show route instance operational

  Operational Routing Instances:
    master
    default

show route instance summary

user@host> show route instance summary

<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>15/0/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iso.0</td>
<td>1/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mpls.0</td>
<td>35/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l3vpn.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inet6.0</td>
<td>2/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l2vpn.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l2circuit.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>BGP-INET</td>
<td>vrf</td>
<td>BGP-INET.inet.0</td>
<td>5/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-INET.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-INET.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>BGP-L</td>
<td>vrf</td>
<td>BGP-L.inet.0</td>
<td>5/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-L.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-L.mpls.0</td>
<td>4/0/0</td>
</tr>
<tr>
<td>Protocol</td>
<td>VRF</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>L2VPN</td>
<td>l2vpn</td>
<td>BGP-L.inet6.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.inet.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.iso.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.inet6.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.l2vpn.0 2/0/0</td>
<td></td>
</tr>
<tr>
<td>LDP</td>
<td>vrf</td>
<td>LDP.inet.0 4/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.iso.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.mpls.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.inet6.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.l2circuit.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td>OSPF</td>
<td>vrf</td>
<td>OSPF.inet.0 7/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSPF.iso.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSPF.inet6.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td>RIP</td>
<td>vrf</td>
<td>RIP.inet.0 6/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIP.iso.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIP.inet6.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td>STATIC</td>
<td>vrf</td>
<td>STATIC.inet.0 4/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>STATIC.iso.0 0/0/0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>STATIC.inet6.0 0/0/0</td>
<td></td>
</tr>
</tbody>
</table>
show route label

List of Syntax  Syntax on page 2392  
Syntax (EX Series Switches) on page 2392

Syntax  
show route label label 
<brief | detail | extensive | terse> 
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  
show route label label 
<brief | detail | extensive | terse>

Release Information  Command introduced before Junos OS Release 7.4. 
Command introduced in Junos OS Release 9.5 for EX Series switches.

Description  Display the routes based on a specified Multiprotocol Label Switching (MPLS) label value.

Options  
label—Value of the MPLS label. 
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.

Required Privilege Level  
view

Related Documentation  
- Example: Configuring Multipoint LDP In-Band Signaling for Point-to-Multipoint LSPs

List of Sample Output  
show route label terse on page 2393  
show route label on page 2393  
show route label detail on page 2393  
show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2393  
show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 2394  
show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 2394  
show route label detail (Dynamic List Next Hop) on page 2395  
show route label extensive on page 2396

Output Fields  
For information about output fields, see the output field table 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 label terse

```bash
user@host> show route label 100016 terse

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 100016</td>
<td>V 170</td>
<td></td>
<td>&gt;10.12.80.1</td>
<td></td>
</tr>
</tbody>
</table>
```

show route label

```bash
user@host> show route label 100016

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

100016 *VPN/170 03:25:41
> to 10.12.80.1 via ge-6/3/2.0, Pop
```

show route label detail

```bash
user@host> show route label 100016 detail

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

100016 (1 entry, 1 announced)
*VPN Preference: 170
Next-hop reference count: 2
Source: 10.12.80.1
Next hop: 10.12.80.1 via ge-6/3/2.0, selected
Label operation: Pop
State: <Active Int Ext>
Local AS: 1
Age: 3:23:31
Task: BGP.0.0.0.0+179
Announcement bits (1): 0-KRT
AS path: 100 I
Ref Cnt: 2
```

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```bash
user@host> show route label 299872 detail

mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
Restart Complete

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
```
Interfaces Fundamentals for Routing Devices

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: 0x2735208
    Next hop: via ge-1/2/22.0
    Next-hop index: 1395
    Load balance label: None;
    Next hop type: Router, Next hop index: 1395
    Address: 0x2736290
    Next-hop reference count: 3

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: 0x9172130
    Next-hop reference count: 3
    Next hop: via so-0/0/3.0
    Next-hop index: 654
    Label operation: Swap 299872
    State: **Active Int>
    Local AS:  1001
    Age: 8:20       Metric: 1
    Task: LDP
    Announcement bits (1): 0-KRT
    AS path: I
    FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1, src 192.168.142.2
    Next hop: via ge-1/2/22.0
    Next-hop index: 1397
    Address: 0x2735d2c
    Next-hop reference count: 3
show route label detail (Dynamic List Next Hop)

The output for `show route label detail` shows the two indirect next hop for an ESI.

```
user@host> show route label 299952 detail

mpls.0: 14 destinations, 14 routes (14 active, 0 holddown, 0 hidden)
299952 (1 entry, 1 announced)
TSI:
KRT in-kernel 299952 /52 -> {Dyn list:indirect(1048577), indirect(1048574)}
  *EVPN Preference: 7
  Next hop type: Dynamic List, Next hop index: 1048575
  Address: 0x13f497fc
  Next-hop reference count: 5
  Next hop: ELNH Address 0xb7a3d90 uflags EVPN data
    Next hop type: Indirect, Next hop index: 0
    Address: 0xb7a3d90
    Next-hop reference count: 3
    Protocol next hop: 10.255.255.2
    Label operation: Push 301344
    Indirect next hop: 0x135b5c00 1048577 INH Session ID: 0x181
      Next hop type: Router, Next hop index: 619
      Address: 0xb7a3d30
      Next-hop reference count: 4
      Next hop: 1.0.0.4 via ge-0/0/1.0
      Label operation: Push 301344, Push 299792(top)
      Label TTL action: no-prop-ttl, no-prop-ttl(top)
      Load balance label: Label 301344: None; Label 299792:
        None;
        Label element ptr: 0xb7a3cc0
        Label parent element ptr: 0xb7a34e0
        Label element references: 1
        Label element child references: 0
        Label element lsp id: 0
        Next hop: ELNH Address 0xb7a37f0 uflags EVPN data
          Next hop type: Indirect, Next hop index: 0
          Address: 0xb7a37f0
          Next-hop reference count: 3
          Protocol next hop: 10.255.255.3
```

Chapter 25: Protocol-Independent Routing Operational Commands

Copyright © 2019, Juniper Networks, Inc. 2395
Label operation: Push 301632
Indirect next hop: 0x135b5480 1048574 INH Session ID: 0x180
   Next hop type: Router, Next hop index: 600
   Address: 0xb7a3790
   Next-hop reference count: 4
   Next hop: 1.0.0.4 via ge-0/0/1.0
Label operation: Push 301632, Push 299776(top)
Label TTL action: no-prop-ttl, no-prop-ttl(top)
Load balance label: Label 301632: None; Label 299776:
None;
   Label element ptr: 0xb7a3720
   Label parent element ptr: 0xb7a3420
   Label element references: 1
   Label element child references: 0
   Label element lsp id: 0
State: <Active Int>
Age: 1:18
Validation State: unverified
Task: evpn global task
Announcement bits (2): 1-KRT 2-evpn global task
AS path: I

show route label extensive

The output for the show route label extensive command is identical to that of the show route label detail command. For sample output, see show route label detail on page 2393.
show route label-switched-path

**List of Syntax**
- Syntax on page 2397
- Syntax (EX Series Switches) on page 2397

**Syntax**
```
show route label-switched-path path-name
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route label-switched-path path-name
  <brief | detail | extensive | terse>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.5 for EX Series switches.

**Description**
Display the routes used in an MPLS label-switched path (LSP).

**Options**
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output.
  - **path-name**—LSP tunnel name.
  - **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 label-switched-path on page 2397

**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 label-switched-path sf-to-ny

inet.0: 29 destinations, 29 routes (29 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.1/32          [MPLS/7] 00:00:06, metric 0
> to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

3.3.3.3/32         *[MPLS/7] 00:00:06, metric 0
> to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```
2.2.2.2/32         *[MPLS/7] 00:00:06, metric 0
        > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

4.4.4.4/32         *[MPLS/7] 00:00:06, metric 0
        to 111.222.1.9 via s0-0/0/0, label-switched-path abc
        > to 111.222.1.9 via s0-0/0/0, label-switched-path xyz
        to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

111.222.1.9/32    *[MPLS/7] 00:00:06, metric 0
        > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

mpls.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both
**show route localization**

**Syntax**

```
show route localization
```

**Release Information**

- Command introduced in Junos OS Release 11.4 for T-Series routers.
- Command introduced in Junos OS Release 12.3 for MX Series routers.

**Description**

(T320, T640, and T1600 routers only) Display route localization details.

**Options**

- `detail`—Display detailed output.

**Required Privilege**

- View

**Related Documentation**

- [Example: Configuring Packet Forwarding Engine FIB Localization](#)

**Output Fields**

Table 182 on page 2399 lists the output fields for the `show route localization` command. Output fields are listed in the approximate order in which they appear.

### Table 182: show route localization Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIB-local</td>
<td>FPCs configured as FIB-local.</td>
</tr>
<tr>
<td>FIB-remote</td>
<td>FPCs configured as FIB-remote.</td>
</tr>
<tr>
<td>Normal</td>
<td>FPCs neither configured as FIB-local or FIB-remote.</td>
</tr>
<tr>
<td>Protocols</td>
<td>IPv4 (inet) or IPv6 (inet6) traffic configured for route localization.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@R0> show route localization
FIB localization ready FPCs (and FIB-local Forwarding Engine addresses)
  FIB-local:  FPC2(4,5)
  FIB-remote: FPC0, FPC1
  Normal:     FPC3, FPC4, FPC5, FPC6, FPC7

user@R0> show route localization detail
FIB localization ready FPCs (and FIB-local Forwarding Engine addresses)
  FIB-local:  FPC2(4,5)
  FIB-remote: FPC0, FPC1
  Normal:     FPC3, FPC4, FPC5, FPC6, FPC7
  FIB localization configuration
```
Protocols: inet, inet6
FIB-local: FPC2
FIB-remote: FPC0, FPC1
Forwarding Engine addresses
  FPC0: 1
  FPC1: 2
  FPC2: 4, 5
  FPC3: 6
  FPC4: 8
  FPC5: 11
  FPC6: 13
  FPC7: 15
**show route martians**

### List of Syntax
Syntax on page 2401  
Syntax (EX Series Switches) on page 2401

### Syntax
show route martians  
<logical-system (all | logical-system-name)>  
<table routing-table-name>

### Syntax (EX Series Switches)
show route martians  
<table routing-table-name>

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

### Description
Display the martian (invalid and ignored) entries associated with each routing table.

### Options
- **none**—Display standard information about route martians for all routing tables.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **table routing-table-name**—(Optional) Display information about route martians for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the `show route martians table inet` command).

### Required Privilege
- **view**

### Related Documentation
- Example: Removing the Class E Prefix on Martian Addresses
- Understanding Martian Addresses

### List of Sample Output
show route martians on page 2402

### Output Fields
Table 183 on page 2401 lists the output fields for the `show route martians` command. Output fields are listed in the approximate order in which they appear.

**Table 183: show route martians Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>table-name</td>
<td>Name of the route table in which the route martians reside.</td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Route destination.</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
### Table 183: `show route martians` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>match value</strong></td>
<td>Route match parameter.</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>Status of the route: allowed or disallowed.</td>
</tr>
</tbody>
</table>

#### Sample Output

```
show route martians

user@host> show route martians

inet.0:
    0.0.0.0/0 exact -- allowed
    0.0.0.0/8 or longer -- disallowed
    127.0.0.0/8 or longer -- disallowed
    192.0.0.0/24 or longer -- disallowed
    240.0.0.0/4 or longer -- disallowed
    224.0.0.0/4 exact -- disallowed
    224.0.0.0/24 exact -- disallowed

inet.1:
    0.0.0.0/0 exact -- allowed
    0.0.0.0/8 or longer -- disallowed
    127.0.0.0/8 or longer -- disallowed
    192.0.0.0/24 or longer -- disallowed
    240.0.0.0/4 or longer -- disallowed

inet.2:
    0.0.0.0/0 exact -- allowed
    0.0.0.0/8 or longer -- disallowed
    127.0.0.0/8 or longer -- disallowed
    192.0.0.0/24 or longer -- disallowed
    240.0.0.0/4 or longer -- disallowed
    224.0.0.0/4 exact -- disallowed
    224.0.0.0/24 exact -- disallowed

inet.3:
    0.0.0.0/0 exact -- allowed
    0.0.0.0/8 or longer -- disallowed
    127.0.0.0/8 or longer -- disallowed
    192.0.0.0/24 or longer -- disallowed
    240.0.0.0/4 or longer -- disallowed
    224.0.0.0/4 exact -- disallowed
    224.0.0.0/24 exact -- disallowed

...  

inet6.0:
    ::1/128 exact -- disallowed
    ff00::/8 exact -- disallowed
    ff02::/16 exact -- disallowed

inet6.1:
    ::1/128 exact -- disallowed
```
<table>
<thead>
<tr>
<th>inet6.2:</th>
<th>inet6.3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>::1/128 exact -- disallowed</td>
<td>::1/128 exact -- disallowed</td>
</tr>
<tr>
<td>ff00::/8 exact -- disallowed</td>
<td>ff00::/8 exact -- disallowed</td>
</tr>
<tr>
<td>ff02::/16 exact -- disallowed</td>
<td>ff02::/16 exact -- disallowed</td>
</tr>
</tbody>
</table>
**show route match-prefix**

**Syntax**

```
show route match-prefix match-prefix;
```

**Release Information**

Command introduced in Junos OS Release 11.4.

**Description**

Allows you to search for routes using regular expressions based on the extended (modern) regular expressions as defined in POSIX 1003.2.

**Options**

- `match-prefix`—Regular expression to match formatted prefix.

**Additional Information**

**Required Privilege**

- Level view

**Related Documentation**

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

**List of Sample Output**

- `show route match-prefix *:10.255.2.200:6:*` (Show all routes matching route distributor 10.255.2.200:6) on page 2404
- `show route match-prefix 7*` (Show all mvpn type-7 routes) on page 2404
- `show route match-prefix *:224.*` (Show all routes matching group 224/4) on page 2404

**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**

```plaintext
user@host> show route match-prefix *:10.255.2.200:6:*

show route match-prefix 7* (Show all mvpn type-7 routes)
user@host> show route table blue.mvpn.0 match-prefix 7*
Paste router command output here

show route match-prefix *:224.* (Show all routes matching group 224/4)
user@host> show route match-prefix *:224.*
```
show route next-hop

List of Syntax  Syntax on page 2405
               Syntax (EX Series Switches) on page 2405

Syntax              show route next-hop next-hop
                   <brief | detail | extensive | terse>
                   <logical-system (all | logical-system-name)>

Syntax (EX Series
Switches)          show route next-hop next-hop
                   <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.

Description       Display the entries in the routing table that are being sent to the specified next-hop
                   address.

Options            brief | detail | extensive | terse—(Optional) Display the specified level of output.
                   logical-system (all | logical-system-name)—(Optional) Perform this operation on all
                   logical systems or on a particular logical system.

next-hop—Next-hop address.

Required Privilege
                   Level
                   view

List of Sample Output
                   show route next-hop on page 2405
                   show route next-hop detail on page 2406
                   show route next-hop extensive on page 2408
                   show route next-hop terse on page 2410

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 next-hop

    user@host> show route next-hop 192.168.71.254

    inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
    Restart Complete
    + = Active Route, - = Last Active, * = Both
show route next-hop detail

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
Restart Complete
10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I
172.16.0.0/12 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

192.168.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

192.168.102.0/23 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

207.17.136.0/24 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

207.17.136.192/32 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
red.inet.0: 4 destinations, 5 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
show route next-hop extensive

user@host> show route next-hop 192.168.71.254 extensive

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.209.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

172.16.0.0/12 (1 entry, 1 announced)
TSI:
KRT in-kernel 172.16.0.0/12 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

192.168.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS: 69
Age: 2:02:28
Task: RT
Announcement bits (1): 0-KRT
AS path: I

192.168.102.0/23 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.102.0/23 -> {192.168.71.254}
*Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS: 69
Age: 2:02:28
Task: RT
Announcement bits (1): 0-KRT
AS path: I

207.17.136.0/24 (1 entry, 1 announced)
TSI:
KRT in-kernel 207.17.136.0/24 -> {192.168.71.254}
*Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS: 69
Age: 2:02:28
Task: RT
Announcement bits (1): 0-KRT
AS path: I

207.17.136.192/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 207.17.136.192/32 -> {192.168.71.254}
*Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS: 69
Age: 2:02:28
Task: RT
Announcement bits (1): 0-KRT
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)
mpls.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
green.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
### show route next-hop terse

**user@host> show route next-hop 192.168.71.254 terse**

**inet.0:** 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)

Restart Complete

+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.10.0.0/16</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 10.209.0.0/16</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 172.16.0.0/12</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 192.168.0.0/16</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 192.168.102.0/23</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 207.17.136.0/24</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 207.17.136.192/32</td>
<td>S</td>
<td>S</td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
</tbody>
</table>

**private1__.inet.0:** 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

**red.inet.0:** 4 destinations, 5 routes (4 active, 0 holddown, 0 hidden)

Restart Complete

**iso.0:** 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

Restart Complete

**mpls.0:** 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

Restart Complete

**inet6.0:** 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

Restart Complete

**private1__.inet6.0:** 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
show route no-community

List of Syntax  Syntax on page 2411
Syntax (EX Series Switches) on page 2411

Syntax  show route no-community
        <brief | detail | extensive | terse>

Syntax (EX Series Switches)  show route no-community
        <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.

Description  Display the route entries in each routing table that are not associated with any community.

Options  none—(Same as brief) Display the route entries in each routing table that are not associated with any community.
        brief | detail | extensive | terse—(Optional) Display the specified level of output.
        logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege  view

List of Sample Output  show route no-community on page 2411
show route no-community detail on page 2412
show route no-community extensive on page 2412
show route no-community terse on page 2413

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 no-community

user@host>  show route no-community
inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.0.0/16       *[Static/5] 00:36:27
                  > to 192.168.71.254 via fxp0.0
show route no-community detail

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 38:08
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 38:08
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

show route no-community extensive

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS:  69
  Age: 2:03:33
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.209.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS:  69
  Age: 2:03:33
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

show route no-community terse

user@host> show route no-community terse

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.10.0.0/16</td>
<td>S 5</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 10.209.0.0/16</td>
<td>S 5</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.52/32</td>
<td>D 0</td>
<td></td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.63/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>&gt;35.1.1.2</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.64/32</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>&gt;35.1.1.2</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.240/32</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.241/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.242/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>* 172.16.12.0/24</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>&gt;so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>* 172.16.14.0/24</td>
<td>0 10</td>
<td>3</td>
<td></td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td>* 172.16.16.0/24</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td>* 172.16.18.0/24</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
</tbody>
</table>
...
show route output

List of Syntax  Syntax on page 2414
Syntax (EX Series Switches) on page 2414

Syntax  show route output (address ip-address | interface interface-name) <brief | detail | extensive | terse> <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route output (address ip-address | interface interface-name) <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.

Description  Display the entries in the routing table learned through static routes and interior gateway protocols that are to be sent out the interface with either the specified IP address or specified name.

To view routes advertised to a neighbor or received from a neighbor for the BGP protocol, use the show route advertising-protocol bgp and show route receive-protocol bgp commands instead.

Options  address ip-address—Display entries in the routing table that are to be sent out the interface with the specified IP address.
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.
interface interface-name—Display entries in the routing table that are to be sent out the interface with the specified name.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege  view

List of Sample Output  show route output address on page 2415
show route output address detail on page 2415
show route output address extensive on page 2416
show route output address terse on page 2416
show route output interface on page 2416
show route output interface detail on page 2417
show route output interface extensive on page 2417
show route output interface terse on page 2417
**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 output address**

```
user@host> show route output address 172.16.36.1/24

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.36.0/24  *[Direct/0] 00:19:56
  > via so-0/1/2.0
  [OSPF/10] 00:19:55, metric 1
  > via so-0/1/2.0

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)

mpls.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

**show route output address detail**

```
user@host> show route output address 172.16.36.1 detail

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
172.16.36.0/24 (2 entries, 0 announced)
  +Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via so-0/1/2.0
  State: <Active Int>
  Age: 23:00
  Task: IF
  AS path: I

OSPF  Preference: 10
  Next-hop reference count: 1
  Next hop: via so-0/1/2.0, selected
  State: <Int>
  Inactive reason: Route Preference
  Age: 22:59
  Metric: 1
  Area: 0.0.0.0
  Task: OSPF
  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)

mpls.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
```
show route output address extensive

The output for the `show route output address extensive` command is identical to that of the `show route output address detail` command. For sample output, see `show route output address detail` on page 2415.

show route output address terse

```
user@host> show route output address 172.16.36.1 terse

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination       P Prf   Metric 1   Metric 2  Next hop        AS path
* 172.16.36.0/24        D   0          >so-0/1/2.0
O  10         1          >so-0/1/2.0

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)
mpls.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```

show route output interface

```
user@host> show route output interface so-0/1/2.0

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.71.240/32   *[OSPF/10] 00:13:00, metric 2
                     via so-0/1/2.0
                     > via so-0/3/2.0
10.255.71.241/32   *[OSPF/10] 00:13:10, metric 1
                     > via so-0/1/2.0
172.16.14.0/24     *[OSPF/10] 00:05:11, metric 3
to 35.1.1.2 via ge-3/1/0.0
                     > via so-0/1/2.0
                     via so-0/3/2.0
172.16.16.0/24     *[OSPF/10] 00:13:10, metric 2
                     > via so-0/1/2.0
172.16.36.0/24     *[Direct/0] 00:13:21
                     > via so-0/1/2.0
                     [OSPF/10] 00:13:20, metric 1
                     > via so-0/1/2.0

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
```
### show route output interface detail

```
inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
10.255.71.240/32 (1 entry, 1 announced)
    *OSPF  Preference: 10
     Next-hop reference count: 2
     Next hop: via so-0/1/2.0
     Next hop: via so-0/3/2.0, selected
     State: <Active Int>
     Age: 14:52      Metric: 2
     Area: 0.0.0.0
     Task: OSPF
     Announcement bits (1): 0-KRT
     AS path: I

10.255.71.241/32 (1 entry, 1 announced)
    *OSPF  Preference: 10
     Next-hop reference count: 4
     Next hop: via so-0/1/2.0, selected
     State: <Active Int>
     Age: 15:02      Metric: 1
     Area: 0.0.0.0
     Task: OSPF
     Announcement bits (1): 0-KRT
     AS path: I

...```

### show route output interface extensive

The output for the `show route output interface extensive` command is identical to that of the `show route output interface detail` command. For sample output, see `show route output interface detail` on page 2417.

### show route output interface terse

```
inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)

+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.255.71.240/32</td>
<td>0</td>
<td>10</td>
<td>2</td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.241/32</td>
<td>0</td>
<td>10</td>
<td>1</td>
<td>&gt;so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td>* 172.16.14.0/24</td>
<td>0</td>
<td>10</td>
<td>3</td>
<td>35.1.1.2</td>
<td></td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Network</th>
<th>Destinations</th>
<th>Routes</th>
<th>Active</th>
<th>Hold Down</th>
<th>Hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>private1__.inet.0</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>iso.0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mpls.0</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inet6.0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>private1__.inet6.0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show route protocol

**List of Syntax**
- Syntax on page 2419
- Syntax (EX Series Switches) on page 2419

**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
  - `dvmrp`—Asynchronous Transfer Mode virtual private network
  - `bgp`—Border Gateway Protocol
  - `ccc`—Circuit cross-connect
  - `direct`—Directly connected route
  - `dvmrp`—Distance Vector Multicast Routing Protocol
  - `esis`—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**  
view

**List of Sample Output**  
show route protocol access on page 2421  
show route protocol access-internal extensive on page 2421  
show route protocol arp on page 2421  
show route protocol bgp on page 2422  
show route protocol bgp detail on page 2422  
show route protocol bgp detail (Labeled Unicast) on page 2423  
show route protocol bgp detail (Aggregate Extended Community Bandwidth) on page 2423  
show route protocol bgp extensive on page 2424  
show route protocol bgp terse on page 2425  
show route protocol direct on page 2425
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)
<table>
<thead>
<tr>
<th>Destination</th>
<th>Protocol</th>
<th>Last Update</th>
<th>Source IP</th>
<th>Source Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.20.1.3/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>20.20.1.4/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.5/32</td>
<td>ARP</td>
<td>00:04:32</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.6/32</td>
<td>ARP</td>
<td>00:04:34</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.7/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.8/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.9/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.10/32</td>
<td>ARP</td>
<td>00:04:35</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.11/32</td>
<td>ARP</td>
<td>00:04:33</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.12/32</td>
<td>ARP</td>
<td>00:04:33</td>
<td>20.20.1.1</td>
<td></td>
</tr>
<tr>
<td>20.20.1.13/32</td>
<td>ARP</td>
<td>00:04:33</td>
<td>20.20.1.1</td>
<td></td>
</tr>
</tbody>
</table>

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, local pref 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)

```
user@host> show route protocol bgp 1.1.1.8/32 detail
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 element child references: 0
  Label element lsp id: 0
  Session Id: 0x140
  Protocol next hop: 1.1.1.1
  Label operation: Push 1000126, Push 1000125, Push 1000124, Push 1000123(top)
  Label TTL action: 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
  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
```

---

**Chapter 25: Protocol-Independent Routing Operational Commands**

---

Copyright © 2019, Juniper Networks, Inc.
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
  Nexthop: 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
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

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
192.168.64.0/21    B 170        100            >172.16.100.1    10023 21 I

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

172.16.8.0/24    *[Direct/0] 17w0d 10:31:49
   > via fe-1/3/1.0
10.255.165.1/32  *[Direct/0] 25w4d 04:13:18
   > via lo0.0
172.16.30.0/24   *[Direct/0] 17w0d 23:06:26
   > via fe-1/3/2.0
192.168.164.0/22 *[Direct/0] 25w4d 04:13:20
   > via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152
   *[Direct/0] 25w4d 04:13:21
   > via lo0.0

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
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 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)
mlps.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
8000001 (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
```
show route protocol ldp

user@host> 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

user@host> 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>
```
show route protocol ospf (Layer 3 VPN)

user@host> show route protocol ospf
```plaintext
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Protocol</th>
<th>Age (Days:Hours:Minutes:Seconds)</th>
<th>Metric</th>
<th>Next Hop Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.39.1.4/30</td>
<td>[OSPF/10]</td>
<td>00:05:18</td>
<td>4</td>
<td>t3-3/2/0.0</td>
</tr>
<tr>
<td>10.39.1.8/30</td>
<td>[OSPF/10]</td>
<td>00:05:18</td>
<td>2</td>
<td>t3-3/2/0.0</td>
</tr>
<tr>
<td>10.255.14.171/32</td>
<td>[OSPF/10]</td>
<td>00:05:18</td>
<td>4</td>
<td>t3-3/2/0.0</td>
</tr>
<tr>
<td>10.255.14.179/32</td>
<td>[OSPF/10]</td>
<td>00:05:18</td>
<td>2</td>
<td>t3-3/2/0.0</td>
</tr>
<tr>
<td>172.16.233.5/32</td>
<td>[OSPF/10]</td>
<td>20:25:55</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Protocol</th>
<th>Age (Days:Hours:Minutes:Seconds)</th>
<th>Metric</th>
<th>Next Hop Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.39.1.16/30</td>
<td>[OSPF/10]</td>
<td>00:05:43</td>
<td>1</td>
<td>so-0/2/2.0</td>
</tr>
<tr>
<td>10.255.14.173/32</td>
<td>[OSPF/10]</td>
<td>00:05:43</td>
<td>1</td>
<td>so-0/2/2.0</td>
</tr>
<tr>
<td>172.16.233.5/32</td>
<td>[OSPF/10]</td>
<td>20:26:20</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Protocol</th>
<th>Age (Days:Hours:Minutes:Seconds)</th>
<th>Metric</th>
<th>Next Hop Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.39.1.16/30</td>
<td>[OSPF/10]</td>
<td>00:05:43</td>
<td>1</td>
<td>so-0/2/2.0</td>
</tr>
<tr>
<td>10.255.14.173/32</td>
<td>[OSPF/10]</td>
<td>00:05:43</td>
<td>1</td>
<td>so-0/2/2.0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Protocol</th>
<th>Age (Days:Hours:Minutes:Seconds)</th>
<th>Metric</th>
<th>Next Hop Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.177/32</td>
<td>[RIP/100]</td>
<td>20:24:34</td>
<td>2</td>
<td>t3-0/2/2.0</td>
</tr>
<tr>
<td>172.16.233.9/32</td>
<td>[RIP/100]</td>
<td>00:03:59</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
```

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
Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
State: <Active Int>
Age: 20:25:02 Metric: 2
Task: VPN-AB-RIPv2
Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179
AS path: I
Route learned from 10.39.1.22 expires in 96 seconds

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

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 route range

List of Syntax  Syntax on page 2433
Syntax (EX Series Switches) on page 2433

Syntax  show route range
        <brief | detail | extensive | terse>
        <destination-prefix>
        <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route range
        <brief | detail | extensive | terse>
        <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 routing table entries using a prefix range.

Options  none—Display standard information about all routing table entries using a prefix range.

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.

destination-prefix—Destination and prefix mask for the range.

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 range on page 2433
                      show route range destination-prefix on page 2434
                      show route range detail on page 2434
                      show route range extensive on page 2435
                      show route range terse on page 2436

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 range

        user@host> show route range
inet.0: 11 destinations, 11 routes (10 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.0.0/16       *[Static/5] 00:30:01
                     > to 192.168.71.254 via fxp0.0
10.209.0.0/16       *[Static/5] 00:30:01
                     > to 192.168.71.254 via fxp0.0
10.255.71.14/32    *[Direct/0] 00:30:01
                     > via lo0.0
172.16.0.0/12      *[Static/5] 00:30:01
                     > to 192.168.71.254 via fxp0.0
192.168.0.0/16     *[Static/5] 00:30:01
                     > to 192.168.71.254 via fxp0.0
192.168.64.0/21    *[Direct/0] 00:30:01
                     > via fxp0.0
192.168.71.14/32   *[Local/0] 00:30:01
                     Local via fxp0.0
192.168.102.0/23   *[Static/5] 00:30:01
                     > to 192.168.71.254 via fxp0.0
...

show route range destination-prefix

user@host> show route range 192.168.0.0/16

inet.0: 11 destinations, 11 routes (10 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.0.0/16       *[Static/5] 00:31:14
                     > to 192.168.71.254 via fxp0.0
192.168.64.0/21    *[Direct/0] 00:31:14
                     > via fxp0.0
192.168.71.14/32   *[Local/0] 00:31:14
                     Local via fxp0.0
192.168.102.0/23   *[Static/5] 00:31:14
                     > to 192.168.71.254 via fxp0.0

show route range detail

user@host> show route range detail

inet.0: 11 destinations, 11 routes (10 active, 0 holddown, 1 hidden)

10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
     Next-hop reference count: 22
     Next hop: 192.168.71.254 via fxp0.0, selected
     State: <Active NoReadvrt Int Ext>
     Age: 30:05
     Task: RT
     Announcement bits (1): 0-KRT
     AS path: I

10.209.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
     Next-hop reference count: 22
     Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Age: 30:05
Task: RT
Announcement bits (1): 0-KRT
AS path: I

10.255.71.14/32 (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>
Age: 30:05
Task: IF
AS path: I

172.16.0.0/12 (1 entry, 1 announced)
*Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Age: 30:05
Task: RT
Announcement bits (1): 0-KRT
AS path: I

...
Next hop type: Interface
Next-hop reference count: 1
Next hop: via lo0.0, selected
State: <Active Int>
Age: 30:17
Task: IF
AS path: I

172.16.0.0/12 (1 entry, 1 announced)
TSI:
KRT in-kernel 172.16.0.0/12 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 30:17
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

...
<table>
<thead>
<tr>
<th>A 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>abcd::10:255:71:14/128</td>
<td>*</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
<tr>
<td>fe80::280:42ff:fe11:226f/128</td>
<td>*</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
</tbody>
</table>

__juniper_private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

+= Active Route, -= Last Active, *= Both

<table>
<thead>
<tr>
<th>A 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>fe80::280:42ff:fe11:226f/128</td>
<td>*</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;lo0.16385</td>
<td></td>
</tr>
</tbody>
</table>
**show route receive-protocol**

**List of Syntax**  
Syntax on page 2438  
Syntax (EX Series Switches) on page 2438

**Syntax**  
show route receive-protocol protocol neighbor-address  
<brief | detail | extensive | terse>  
logical-system (all | logical-system-name)

**Syntax (EX Series Switches)**  
show route receive-protocol protocol neighbor-address  
<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.

**Description**  
Display the routing information as it was received through a particular neighbor using a particular dynamic routing protocol.

**Options**  
brief | detail | extensive | terse—(Optional) Display the specified level of output.  
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.  
protocol neighbor-address—Protocol transmitting the route (bgp, dvmrp, msdp, pim, rip, or ripng) and address of the neighboring router from which the route entry was received.

**Additional Information**  
The output displays the selected routes and the attributes with which they were received, but does not show the effects of import policy on the routing attributes.

**Required Privilege Level**  
view

**List of Sample Output**  
show route receive-protocol bgp on page 2441  
show route receive-protocol bgp extensive on page 2441  
show route receive-protocol bgp table extensive on page 2442  
show route receive-protocol bgp logical-system extensive on page 2442  
show route receive-protocol bgp detail (Layer 2 VPN) on page 2443  
show route receive-protocol bgp extensive (Layer 2 VPN) on page 2443  
show route receive-protocol bgp (Layer 3 VPN) on page 2444  
show route receive-protocol bgp detail (Layer 3 VPN) on page 2444  
show route receive-protocol bgp detail (Long-Lived Graceful Restart) on page 2445  
show route receive-protocol bgp detail (Labeled Unicast) on page 2446  
show route receive-protocol bgp extensive (Layer 3 VPN) on page 2446  
Show route receive protocol (Segment Routing Traffic Engineering) on page 2447
Output Fields  Table 184 on page 2439 describes the output fields for the show route receive-protocol command. Output fields are listed in the approximate order in which they appear.

Table 184: show route receive-protocol Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table—for example, inet.0.</td>
<td>All levels</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>states:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• holddown (routes that are in pending state before being declared inactive)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>Destination prefix.</td>
<td>none brief</td>
</tr>
<tr>
<td>MED</td>
<td>Multiple exit discriminator value included in the route.</td>
<td>none brief</td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Destination prefix. The entry value is the number of routes for this destination,</td>
<td>detail extensive</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td>and the announced value is the number of routes being announced for this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>destination.</td>
<td></td>
</tr>
<tr>
<td>Accepted</td>
<td>The LongLivedStale flag indicates that the route was marked LLGR-stale by</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LongLivedStale</td>
<td>this router, as part of the operation of LLGR receiver mode. Either this flag or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the LongLivedStaleImport flag may be displayed for a route. Neither of these</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flags are displayed at the same time as the Stale (ordinary GR stale) flag.</td>
<td></td>
</tr>
<tr>
<td>Accepted</td>
<td>The LongLivedStaleImport flag indicates that the route was marked LLGR-stale</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LongLivedStaleImport</td>
<td>when it was received from a peer, or by import policy. Either this flag or the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LongLivedStale flag may be displayed for a route. Neither of these flags are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>displayed at the same time as the Stale (ordinary GR stale) flag.</td>
<td></td>
</tr>
<tr>
<td>ImportAccepted</td>
<td>Accept all received BGP long-lived graceful restart (LLGR) and LLGR stale</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LongLivedStaleImport</td>
<td>routes learned from configured neighbors and imported into the inet.0 routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>table</td>
<td></td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>64-bit prefix added to IP subnets to make them unique.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>device uses this first label when sending traffic toward the advertising PE routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device.</td>
<td></td>
</tr>
</tbody>
</table>
Table 184: show route receive-protocol Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Label</td>
<td>Virtual private network (VPN) label. Packets are sent between CE and PE routing</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>devices by advertising VPN labels. VPN labels transit over either an RSVP or an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LDP label-switched path (LSP) tunnel.</td>
<td></td>
</tr>
<tr>
<td>Next hop</td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>selected route.</td>
<td></td>
</tr>
<tr>
<td>Localpref or Lclpref</td>
<td>Local preference value included in the route.</td>
<td>All levels</td>
</tr>
<tr>
<td>AS path</td>
<td>Autonomous system (AS) path through which the route was learned. The letters</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>at the end of the AS path indicate the path origin, providing an indication of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>state of the route at the point at which the AS path originated:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When AS path numbers are included in the route, the format is as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• [ ]—Brackets enclose the number that precedes the AS path. This number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>represents the number of ASs present in the AS path, when calculated as</td>
<td></td>
</tr>
<tr>
<td></td>
<td>defined in RFC 4271. This value is used the AS-path merge process, as defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in RFC 4893.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• [ ]—If more than one AS number is configured on the router, or if AS path</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prepending is configured, brackets enclose the local AS number associated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with the AS path.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• {}—Braces enclose AS sets, which are groups of AS numbers in which the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>order does not matter. A set commonly results from route aggregation. The</td>
<td></td>
</tr>
<tr>
<td></td>
<td>numbers in each AS set are displayed in ascending order.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ()—Parentheses enclose a confederation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ( [ ] )—Parentheses and brackets enclose a confederation set.</td>
<td></td>
</tr>
<tr>
<td>NOTE:</td>
<td>In Junos OS Release 10.3 and later, the AS path field displays an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unrecognized attribute and associated hexadecimal value if BGP receives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attribute 128 (attribute set) and you have not configured an independent domain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in any routing instance.</td>
<td></td>
</tr>
<tr>
<td>Route Labels</td>
<td>Stack of labels carried in the BGP route update.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Cluster list</td>
<td>(For route reflected output only) Cluster ID sent by the route reflector.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Originator ID</td>
<td>(For route reflected output only) Address of routing device that originally sent</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Communities</td>
<td>the route to the route reflector.</td>
<td></td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See the Output Field table in the show</td>
<td></td>
</tr>
<tr>
<td></td>
<td>route detail command for all possible values for this field.</td>
<td></td>
</tr>
<tr>
<td>AIGP</td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Attrset AS</td>
<td>Number, local preference, and path of the AS that originated the route. These</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>values are stored in the Attrset attribute at the originating routing device.</td>
<td></td>
</tr>
</tbody>
</table>
Table 184: show route receive-protocol Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer2-info:encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

**show route receive-protocol bgp**

```
user@host> show route receive-protocol bgp 10.255.245.215
inet.0: 28 destinations, 33 routes (27 active, 0 holddown, 1 hidden)
Prefix Next hop MED Lclpref AS path
10.22.1.0/24 10.255.245.215 0 100 I
10.22.2.0/24 10.255.245.215 0 100 I
```

**show route receive-protocol bgp extensive**

```
user@host> show route receive-protocol bgp 10.255.245.63 extensive
inet.0: 244 destinations, 244 routes (243 active, 0 holddown, 1 hidden)
Prefix Next hop MED Lclpref AS path
172.16.1.0/24 (1 entry, 1 announced)
  Next hop: 10.0.50.3
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.45
172.16.163.0/16 (1 entry, 1 announced)
  Next hop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.68
172.16.164.0/16 (1 entry, 1 announced)
  Next hop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.45
172.16.195.0/24 (1 entry, 1 announced)
  Next hop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.68
inet.2: 63 destinations, 63 routes (63 active, 0 holddown, 0 hidden)
Prefix Next hop MED Lclpref AS path
inet.3: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix Next hop MED Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
```
show route receive-protocol bgp table extensive

user@host> show route receive-protocol bgp 207.17.136.192 table inet.0 66.117.68.0/24 extensive

inet.0: 227315 destinations, 227316 routes (227302 active, 0 holddown, 13 hidden)
* 66.117.63.0/24 (1 entry, 1 announced)
   Nexthop: 207.17.136.29
   Localpref: 100
   AS path: AS2 PA[6]: 14203 2914 3356 29748 33437 AS_TRANS
   AS path: AS4 PA[2]: 33437 393219
   AS path: Merged[6]: 14203 2914 3356 29748 33437 393219
   Communities: 2914:420

show route receive-protocol bgp logical-system extensive

user@host> show route receive-protocol bgp 10.0.0.9 logical-system PE4 extensive

inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)
* 10.0.0.0/30 (1 entry, 1 announced)
   Accepted
   Route Label: 3
   Nexthop: 10.0.0.9
   AS path: 13979 I

* 10.0.0.4/30 (1 entry, 1 announced)
   Accepted
   Route Label: 3
   Nexthop: 10.0.0.9
   AS path: 13979 I

10.0.0.8/30 (2 entries, 1 announced)
   Accepted
   Route Label: 3
   Nexthop: 10.0.0.9
   AS path: 13979 I

* 10.9.9.1/32 (1 entry, 1 announced)
   Accepted
   Route Label: 3
   Nexthop: 10.0.0.9
   AS path: 13979 I

* 10.100.1.1/32 (1 entry, 1 announced)
   Accepted
   Route Label: 3
   Nexthop: 10.0.0.9
   AS path: 13979 I

* 172.16.44.0/24 (1 entry, 1 announced)
   Accepted
   Route Label: 300096
   Nexthop: 10.0.0.9
   AS path: 13979 I
   AIGP: 203

* 172.16.55.0/24 (1 entry, 1 announced)
show route receive-protocol bgp detail (Layer 2 VPN)

user@host> show route receive-protocol bgp 10.255.14.171 detail

inet.0: 68 destinations, 68 routes (67 active, 0 holddown, 1 hidden)
Prefix Nexthop MED Lclpref AS path
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
mpls.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
frame-vpn.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 1 announced)
Route Distinguisher: 10.255.245.35:1
Label-base : 800000, range : 4, status-vector : 0x0
Nexthop: 10.255.245.35
Localpref: 100
AS path: I
Communities: target:65299:100 Layer2-info: encaps:FRAME RELAY,
control flags: 0, mtu: 0
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 0 announced)
Route Distinguisher: 10.255.245.35:1
Label-base : 800000, range : 4, status-vector : 0x0
Nexthop: 10.255.245.35
Localpref: 100
AS path: I
Communities: target:65299:100 Layer2-info: encaps:FRAME RELAY,
control flags:0, mtu: 0

show route receive-protocol bgp extensive (Layer 2 VPN)

user@host> show route receive-protocol bgp 10.255.14.171 extensive

inet.0: 68 destinations, 68 routes (67 active, 0 holddown, 1 hidden)
Prefix Nexthop MED Lclpref AS path
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
show route receive-protocol bgp (Layer 3 VPN)

user@host> show route receive-protocol bgp 10.255.14.171

inet.0: 33 destinations, 33 routes (32 active, 0 holddown, 1 hidden)
Prefix Nexthop MED Lc1pref AS path
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path
VPN-A.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path
VPN-B.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path
mpls.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path
bgp-13vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lc1pref AS path

show route receive-protocol bgp detail (Layer 3 VPN)

user@host> show route receive-protocol bgp 10.255.14.174 detail
inet.0: 16 destinations, 17 routes (15 active, 0 holddown, 1 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
vpna.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
* 10.49.0.0/30 (1 entry, 1 announced)
  Route Distinguisher: 10.255.14.176:2
  VPN Label: 101264
  Nexthop: 10.255.14.174
  Localpref: 100
  AS path: I
  Communities: target:200:100
  AttrSet AS: 100
    Localpref: 100
    AS path: I
* 10.255.14.172/32 (1 entry, 1 announced)
  Route Distinguisher: 10.255.14.176:2
  VPN Label: 101280
  Nexthop: 10.255.14.174
  Localpref: 100
  AS path: I
  Communities: target:200:100
  AttrSet AS: 100
    Localpref: 100
    AS path: I
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
* 10.255.14.174:2:10.49.0.0/30 (1 entry, 0 announced)
  Route Distinguisher: 10.255.14.176:2
  VPN Label: 101264
  Nexthop: 10.255.14.174
  Localpref: 100
  AS path: I
  Communities: target:200:100
  AttrSet AS: 100
    Localpref: 100
    AS path: I
  Route Distinguisher: 10.255.14.176:2
  VPN Label: 101280
  Nexthop: 10.255.14.174
  Localpref: 100
  AS path: I
  Communities: target:200:100
  AttrSet AS: 100
    Localpref: 100
    AS path: I
inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

show route receive-protocol bgp detail (Long-Lived Graceful Restart)

user@host> show route receive-protocol bgp 10.4.12.11 detail

bgp.l2vpn.0: 38 destinations, 39 routes (37 active, 0 holddown, 1 hidden)
* 172.16.1.4:100:172.16.1.4/96 AD (1 entry, 1 announced)
  Accepted LongLivedStale LongLivedStaleImport
  Nexthop: 10.4.12.11
  Localpref: 100
  AS path: I
show route receive-protocol bgp detail (Labeled Unicast)

user@host> show route receive-protocol bgp detail
inet.0: 45 destinations, 46 routes (45 active, 0 holddown, 0 hidden)
  * 1.1.1.8/32 (2 entries, 2 announced)
    Accepted
    Route Labels: 1000123(top) 1000124 1000125 1000126
    Nexthop: 1.1.1.4
    Localpref: 100
    AS path: I
    Entropy label capable, next hop field matches route next hop
inet.3: 15 destinations, 21 routes (6 active, 0 holddown, 14 hidden)
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
inet6.0: 26 destinations, 28 routes (26 active, 0 holddown, 0 hidden)
  * 100::1/128 (2 entries, 2 announced)
    Accepted
    Route Labels: 1000123(top) 1000124 1000125 1000126
    Nexthop: ::ffff:1.1.1.4
    Localpref: 100
    AS path: I
    Entropy label capable, next hop field matches route next hop
inet6.3: 22 destinations, 23 routes (22 active, 0 holddown, 0 hidden)

show route receive-protocol bgp extensive (Layer 3 VPN)

user@host> show route receive-protocol bgp extensive
inet.0: 244 destinations, 244 routes (243 active, 0 holddown, 1 hidden)
  Prefix  Nexthop  MED  Lclpref  AS path
  172.16.1.0/24 (1 entry, 1 announced)
    Nexthop: 10.0.50.3
    Localpref: 100
    AS path: I <Originator>
    Cluster list: 10.2.3.1
    Originator ID: 10.255.245.45
  172.16.163.0/16 (1 entry, 1 announced)
    Nexthop: 111.222.5.254
    Localpref: 100
    AS path: I <Originator>
    Cluster list: 10.2.3.1
    Originator ID: 10.255.245.68
  172.16.164.0/16 (1 entry, 1 announced)
    Nexthop: 111.222.5.254
    Localpref: 100
    AS path: I <Originator>
    Cluster list: 10.2.3.1
    Originator ID: 10.255.245.68
  172.16.195.0/24 (1 entry, 1 announced)
    Nexthop: 111.222.5.254
    Localpref: 100
    AS path: I <Originator>
    Cluster list: 10.2.3.1
    Originator ID: 10.255.245.68
inet.2: 63 destinations, 63 routes (63 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
inet.3: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
mpls.0: 48 destinations, 48 routes (48 active, 0 holddown, 0 hidden)

Show route receive protocol (Segment Routing Traffic Engineering)

show route receive protocol bgp 10.1.1.4
bgp.inetcolor.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
* 50-4.4.4.4-1234<sr6>/96 (1 entry, 0 announced)
  Import Accepted
  Distinguisher: 50
  Color: 1234
  Nexthop: 10.1.1.4
  Localpref: 100
  AS path: 3 I
  Communities: target:1.1.1.1:1

inetcolor.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
* 4.4.4.4-1234<c6>/64 (1 entry, 1 announced)
  Import Accepted
  Color: 1234
  Nexthop: 10.1.1.4
  Localpref: 100
  AS path: 3 I
  Communities: target:1.1.1.1:1

user@host# run show route receive-protocol bgp 5001:1::4
bgp.inet6color.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
* 50-2001:1::4-1234<sr6>/192 (1 entry, 0 announced)
  Import Accepted
  Distinguisher: 50
  Color: 1234
  Nexthop: ::ffff:1.1.1.4
  Localpref: 100
  AS path: 3 I
  Communities: target:1.1.1.1:1

inet6color.0: 6 destinations, 7 routes (6 active, 0 holddown, 0 hidden)
* 2001::5-1234<c6>/160 (1 entry, 1 announced)
  Import Accepted
  Color: 1234
  Nexthop: ::ffff:1.1.1.5
  Localpref: 100
  AS path: 3 I
  Communities: target:2:1
**show route resolution**

**List of Syntax**

Syntax (EX Series Switches) on page 2448

**Syntax**

```
show route resolution
  <brief | detail | extensive | summary>
  <index index>
  <logical-system (all | logical-system-name)>
  <prefix>
  <table routing-table-name>
  <unresolved>
```

**Syntax (EX Series Switches)**

```
show route resolution
  <brief | detail | extensive | summary>
  <index index>
  <prefix>
  <table routing-table-name>
  <unresolved>
```

**Release Information**

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

**Description**

Display the entries in the next-hop resolution database. This database provides for recursive resolution of next hops through other prefixes in the routing table.

**Options**

- `none`—Display standard information about all entries in the next-hop resolution database.
- `brief | detail | extensive | summary`—(Optional) Display the specified level of output.
- `index index`—(Optional) Show the index of the resolution tree.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `prefix network/destination-prefix`—(Optional) Display database entries for the specified address.
- `table routing-table-name`—(Optional) Display information about a particular routing table (for example, `inet.0`) where policy-based export is currently enabled.
- `unresolved`—(Optional) Display routes that could not be resolved.

**Required Privilege Level**

view

**Related Documentation**

- Example: Configuring Route Resolution on PE Routers
List of Sample Output

- show route resolution detail on page 2450
- show route resolution (Multipath Resolution) on page 2451
- show route resolution summary on page 2452
- show route resolution unresolved on page 2452
### Output Fields

Table 185 on page 2450 describes the output fields for the `show route resolution` command. Output fields are listed in the approximate order in which they appear.

#### Table 185: show route resolution 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 whose prefixes are resolved using the entries in the route resolution database. For routing table groups, this is the name of the primary routing table whose prefixes are resolved using the entries in the route resolution database.</td>
</tr>
<tr>
<td>Tree index</td>
<td>Tree index identifier.</td>
</tr>
<tr>
<td>Nodes</td>
<td>Number of nodes in the tree.</td>
</tr>
<tr>
<td>Reference count</td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td>Contributing routing tables</td>
<td>Routing tables used for next-hop resolution.</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 <code>inet.0</code> resolving through <code>inet.0</code> and <code>inet.3</code>, this field indicates which routing table, <code>inet.0</code> or <code>inet.3</code>, provided the best path for a particular prefix.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric associated with the forwarding next hop.</td>
</tr>
<tr>
<td>Node path count</td>
<td>Number of nodes in the path.</td>
</tr>
<tr>
<td>Forwarding next hops</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>
<tr>
<td>Merged</td>
<td>Merged—Merged next hops when recursive resolution of multipath is configured.</td>
</tr>
</tbody>
</table>

### Sample Output

**show route resolution detail**

```
user@host> show route resolution detail

Tree Index: 1, Nodes 0, Reference Count 1
Contributing routing tables: inet.3
Tree Index: 2, Nodes 23, Reference Count 1
Contributing routing tables: inet.0 inet.3
10.10.0.0/16 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 1
10.10.1.0/30 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 1
10.31.1.1/32 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 0
10.31.1.4/30 Originating RIB: inet.0
```
show route resolution (Multipath Resolution)

user@host> show route resolution detail
user@host> show route resolution detail 10.1.1.2
Tree Index: 1, Nodes 36, Reference Count 3
Contributing routing tables: inet.0 inet.3
Policy: [ abc ]
10.1.1.2/32 Originating RIB: inet.0
Node path count: 1
Next hop subtype: INDIRECT
Indirect next hops: 2
Protocol next hop: 10.1.1.1
Inode flags: 0x206 path flags: 0x08
Path fnh link: 0xc9321c0 path inh link: 0x0
Indirect next hop: 0xb2b20f0 1048574 INH Session ID: 0x143
Indirect path forwarding next hops: 1
   Next hop type: Router
   Next hop: 12.1.1.2 via ge-2/0/1.0 Session Id: 0x144
   Next hop: 13.1.1.2 via ge-2/0/2.0 Session Id: 0x145

10.1.1.1/32 Originating RIB: inet.0
Node path count: 1
Node flags: 1
Forwarding nexthops: 1 (Merged)
Nexthop: 12.1.1.2 via ge-2/0/1.0
Nexthop: 13.1.1.2 via ge-2/0/2.0

user@host> show route resolution summary
Tree Index: 1, Nodes 7, Reference Count 2
Contributing routing tables: inet.3
Tree Index: 2, Nodes 7, Reference Count 8213
Contributing routing tables: inet.3
Policy: [ RRwM ]
Tree Index: 3, Nodes 7, Reference Count 2
Contributing routing tables: inet6.3
Tree Index: 4, Nodes 1, Reference Count 1
Contributing routing tables: iso.0
Tree Index: 5, Nodes 1000061, Reference Count 13
Contributing routing tables: inet.0 inet.3
Policy: [ Community-RRwM ]
Tree Index: 6, Nodes 2013, Reference Count 6
Contributing routing tables: inet6.0 inet6.3
show route resolution summary

user@host> show route resolution summary

Tree Index 1, Nodes 24, Reference Count 1
Contributing routing tables: :voice.inet.0 :voice.inet.3
Tree Index 2, Nodes 2, Reference Count 1
Contributing routing tables: inet.3
Tree Index 3, Nodes 43, Reference Count 1
Contributing routing tables: inet.0 inet.3

show route resolution unresolved

user@host> show route resolution unresolved

Tree Index 1
vt-3/2/0.32769.0 /16
    Protocol Nexthop: 10.255.71.238 Push 800000
    Indirect nexthop: 0 -
vt-3/2/0.32772.0 /16
    Protocol Nexthop: 10.255.70.103 Push 800008
    Indirect nexthop: 0 -
Tree Index 2
**show route snooping**

**Syntax**
```
show route snooping
    <brief | detail | extensive | terse>
    <all>
    <best address/prefix>
    <exact address>
    <logical-system logical-system-name>
    <range prefix-range>
    <summary>
    <table table-name>
```

**Release Information**
Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the entries in the routing table that were learned from snooping.

**Options**
- `none`—Display the entries in the routing table that were learned from snooping.
- `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`.
- `all`—(Optional) Display all entries, including hidden entries.
- `best address/prefix`—(Optional) Display the longest match for the provided address and optional prefix.
- `exact address/prefix`—(Optional) Display exact matches for the provided address and optional prefix.
- `logical-system logical-system-name`—(Optional) Display information about a particular logical system, or type `all`.
- `range prefix-range`—(Optional) Display information for the provided address range.
- `summary`—(Optional) Display route snooping summary statistics.
- `table table-name`—(Optional) Display information for the named table.

**Required Privilege Level**
`view`

**List of Sample Output**
- `show route snooping detail on page 2454`
- `show route snooping logical-system all on page 2454`

**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 snooping detail

user@host> show route snooping detail

__+domainAll__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

224.0.0.2/32 (1 entry, 1 announced)
  *IGMP Preference: 0
  Next hop type: MultiRecv
  Next-hop reference count: 4
  State: <Active NoReadvrt Int>
  Age: 2:24
  Task: IGMP
  Announcement bits (1): 0-KRT
  AS path: I

224.0.0.22/32 (1 entry, 1 announced)
  *IGMP Preference: 0
  Next hop type: MultiRecv
  Next-hop reference count: 4
  State: <Active NoReadvrt Int>
  Age: 2:24
  Task: IGMP
  Announcement bits (1): 0-KRT
  AS path: I

__+domainAll__.inet.1: 36 destinations, 36 routes (36 active, 0 holddown, 0 hidden)

224.0.0.0.0.0.0.0/24 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4), Next hop index: 1048584
  Next-hop reference count: 4
  State: <Active Int>
  Age: 2:24
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

show route snooping logical-system all

user@host> show route snooping logical-system all

logical-system: default

inet.1: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
Restart Unsupported
+ = Active Route, - = Last Active, * = Both

0.0.0.1.0.0.232.1.1.65,100.1.1.2/112*[Multicast/180] 00:07:36
  Multicast (IPv4) Composite

0.0.0.1.0.0.232.1.1.66,100.1.1.2/112*[Multicast/180] 00:07:36
  Multicast (IPv4) Composite

0.0.0.1.0.0.232.1.1.67,100.1.1.2/112*[Multicast/180] 00:07:36

<snip>
default-switch.inet.1: 237 dest, 237 rts (237 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
0.15,0.1,0.0,0.0.0.0,0.0.0.0,2/120*[Multicast/180] 00:08:21
   Multicast (IPv4) Composite
0.15,0.1,0.0,0.0.0.0,0.0.0.0,2.17/128*[Multicast/180] 00:08:21
   Multicast (IPv4) Composite

<snip>
show route source-gateway

List of Syntax  Syntax on page 2456  
Syntax (EX Series Switches) on page 2456

Syntax  show route source-gateway address  
<brief | detail | extensive | terse>  
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route source-gateway address  
<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.

Description  Display the entries in the routing table that were learned from a particular address. The Source field in the show route detail command output lists the source for each route, if known.

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.

address—IP address of the system.

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 source-gateway on page 2456  
show route source-gateway detail on page 2457  
show route source-gateway extensive on page 2459

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 source-gateway

user@host> show route source-gateway 10.255.70.103
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)  
Restart Complete
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

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)
Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96
* [BGP/170] 12:12:24, localpref 100, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

10.255.70.103:2:3:1/96
* [BGP/170] 12:12:24, localpref 0, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

show route source-gateway detail

user@host>  show route source-gateway 10.255.70.103 detail

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

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)
Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
Restart Complete

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
* BGP    Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS:    69 Peer AS:    69
  Age: 12:14:00   Metric2: 1
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-green-l2vpn
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
               control flags: , mtu: 0
  Label-base: 800008, range: 8
  Localpref: 100
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:2:3:1/96 (1 entry, 1 announced)
* BGP    Preference: 170/-1
  Route Distinguisher: 10.255.70.103:2
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS:    69 Peer AS:    69
  Age: 12:14:00   Metric2: 1
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-red-l2vpn
  AS path: I
  Communities: target:11111:2 Layer2-info: encaps:VPLS,
               control flags:Site-Down, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 0
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 0 announced)
* BGP    Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
show route source-gateway extensive

user@host> show route source-gateway 10.255.70.103 extensive

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

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)
Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
Restart Complete

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
Next-hop reference count: 7
Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 12:15:24  Metric2: 1
Task: BGP_69.10.255.70.103+179
Announcement bits (1): 0-green-l2vpn
AS path: I
Communities: target:1111:1 Layer2-info: encaps:VPLS,
control flags:, mtu: 0
Label-base: 800008, range: 8
Localpref: 100
Router ID: 10.255.70.103
Primary Routing Table bgp.l2vpn.0

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:2:3:1/96 (1 entry, 1 announced)
  *BGP  Preference: 170/-1
  Route Distinguisher: 10.255.70.103:2
Next-hop reference count: 7
Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 12:15:24  Metric2: 1
Task: BGP_69.10.255.70.103+179
Announcement bits (1): 0-red-l2vpn
AS path: I
Communities: target:1111:2 Layer2-info: encaps:VPLS,
control flags:Site-Down, mtu: 0
Label-base: 800016, range: 8
Localpref: 0
Router ID: 10.255.70.103
Primary Routing Table bgp.l2vpn.0

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 0 announced)
  *BGP  Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
Next-hop reference count: 7
Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 12:15:24  Metric2: 1
Task: BGP_69.10.255.70.103+179
AS path: I
Communities: target:1111:1 Layer2-info: encaps:VPLS,
control flags:, mtu: 0
Label-base: 800008, range: 8
Localpref: 100
Router ID: 10.255.70.103

Copyright © 2019, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Tables: green.l2vpn.0</td>
<td></td>
</tr>
<tr>
<td>Indirect next hops: 1</td>
<td></td>
</tr>
<tr>
<td>Protocol next hop: 10.255.70.103 Metric: 2</td>
<td></td>
</tr>
<tr>
<td>Indirect next hop: 2 no-forward</td>
<td></td>
</tr>
<tr>
<td>Indirect path forwarding next hops: 1</td>
<td></td>
</tr>
<tr>
<td>Next hop: via so-0/3/0.0 weight 0x1</td>
<td></td>
</tr>
<tr>
<td>10.255.70.103/32 Originating RIB: inet.3</td>
<td></td>
</tr>
<tr>
<td>Metric: 2</td>
<td></td>
</tr>
<tr>
<td>Node path count: 1</td>
<td></td>
</tr>
<tr>
<td>Forwarding nexthops: 1</td>
<td></td>
</tr>
<tr>
<td>Nexthop: via so-0/3/0.0</td>
<td></td>
</tr>
<tr>
<td>*BGP Preference: 170/-1</td>
<td></td>
</tr>
<tr>
<td>Route Distinguisher: 10.255.70.103:2</td>
<td></td>
</tr>
<tr>
<td>Next-hop reference count: 7</td>
<td></td>
</tr>
<tr>
<td>Source: 10.255.70.103</td>
<td></td>
</tr>
<tr>
<td>Protocol next hop: 10.255.70.103</td>
<td></td>
</tr>
<tr>
<td>Indirect next hop: 2 no-forward</td>
<td></td>
</tr>
<tr>
<td>State: &lt;Active Int Ext&gt;</td>
<td></td>
</tr>
<tr>
<td>Local AS: 69</td>
<td>Peer AS: 69</td>
</tr>
<tr>
<td>Age: 12:15:24</td>
<td>Metric2: 1</td>
</tr>
<tr>
<td>Task: BGP_69.10.255.70.103+179</td>
<td></td>
</tr>
<tr>
<td>AS path: I</td>
<td></td>
</tr>
<tr>
<td>Communities: target:11111:2 Layer2-info: VPLS, control flags:Site-Down, mtu: 0</td>
<td></td>
</tr>
<tr>
<td>Label-base: 800016, range: 8</td>
<td></td>
</tr>
<tr>
<td>Localpref: 0</td>
<td></td>
</tr>
<tr>
<td>Router ID: 10.255.70.103</td>
<td></td>
</tr>
<tr>
<td>Secondary Tables: red.l2vpn.0</td>
<td></td>
</tr>
<tr>
<td>Indirect next hops: 1</td>
<td></td>
</tr>
<tr>
<td>Protocol next hop: 10.255.70.103 Metric: 2</td>
<td></td>
</tr>
<tr>
<td>Indirect next hop: 2 no-forward</td>
<td></td>
</tr>
<tr>
<td>Indirect path forwarding next hops: 1</td>
<td></td>
</tr>
<tr>
<td>Next hop: via so-0/3/0.0 weight 0x1</td>
<td></td>
</tr>
<tr>
<td>10.255.70.103/32 Originating RIB: inet.3</td>
<td></td>
</tr>
<tr>
<td>Metric: 2</td>
<td></td>
</tr>
<tr>
<td>Node path count: 1</td>
<td></td>
</tr>
<tr>
<td>Forwarding nexthops: 1</td>
<td></td>
</tr>
<tr>
<td>Nexthop: via so-0/3/0.0</td>
<td></td>
</tr>
</tbody>
</table>
**show route summary**

**List of Syntax**  
Syntax on page 2462  
Syntax (EX Series Switches) on page 2462

**Syntax**  
`show route summary`  
`<logical-system (all | logical-system-name)>`  
`<table routing-table-name>`

**Syntax (EX Series Switches)**  
`show route summary`

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

**Description**  
Display summary statistics about the entries in the routing table.

CPU utilization might increase while the device learns routes. We recommend that you use the `show route summary` command after the device learns and enters the routes into the routing table. Depending on the size of your network, this might take several minutes. If you receive a “timeout communicating with routing daemon” error when using the `show route summary` command, wait several minutes before attempting to use the command again. This is not a critical system error, but you might experience a delay in using the command-line interface (CLI).

**Options**  
`none`—Display summary statistics about the entries in the routing table.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

`table routing-table-name`—(Optional) Display summary statistics for all routing tables whose name begins with this string (for example, `inet.0` and `inet6.0` are both displayed when you run the `show route summary table inet` command). If you only want to display statistics for a specific routing table, make sure to enter the exact name of that routing table.

**Required Privilege Level**  
`view`

**List of Sample Output**  
`show route summary` on page 2464  
`show route summary table` on page 2464  
`show route summary table (with Route Limits Configured for the Routing Table)` on page 2465

**Output Fields**  
Table 186 on page 2463 lists the output fields for the `show route summary` command. Output fields are listed in the approximate order in which they appear.
**Table 186: show route summary Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Address of the local routing device.</td>
</tr>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, <code>inet.0</code>).</td>
</tr>
<tr>
<td>destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>routes</td>
<td>Number of routes in the routing table:</td>
</tr>
<tr>
<td></td>
<td>• active—Number of routes that are active.</td>
</tr>
<tr>
<td></td>
<td>• holddown—Number of routes that are in the hold-down state before being declared inactive.</td>
</tr>
<tr>
<td></td>
<td>• hidden—Number of routes that are not used because of routing policy.</td>
</tr>
<tr>
<td>Restart complete</td>
<td>All protocols have restarted for this routing table.</td>
</tr>
<tr>
<td>Restart state:</td>
<td>Restart state:</td>
</tr>
<tr>
<td></td>
<td>• Pending: protocol-name—List of protocols that have not yet completed graceful restart for this routing table.</td>
</tr>
<tr>
<td></td>
<td>• Complete—All protocols have restarted for this routing table.</td>
</tr>
<tr>
<td></td>
<td>For example, if the output shows-</td>
</tr>
<tr>
<td></td>
<td>• LDP.inet.0: 5 routes (4 active, 1 holddown, 0 hidden)</td>
</tr>
<tr>
<td></td>
<td>Restart Pending: OSPF LDP VPN</td>
</tr>
<tr>
<td></td>
<td>This indicates that OSPF, LDP, and VPN protocols did not restart for LDP.inet.0 routing table.</td>
</tr>
<tr>
<td></td>
<td>• vpls_1.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)</td>
</tr>
<tr>
<td></td>
<td>Restart Complete</td>
</tr>
<tr>
<td></td>
<td>This indicates that all protocols have restarted for vpls_1.l2vpn.0 routing table.</td>
</tr>
<tr>
<td>Limit/Threshold</td>
<td>Displays the configured route limits for the routing table set with the <code>maximum-prefixes</code> and the <code>maximum-paths</code> statements. If you do not configure route limits for the routing table, the show output does not display this information.</td>
</tr>
<tr>
<td></td>
<td>• destinations—The first number represents the maximum number of route prefixes installed in the routing table. The second number represents the number of route prefixes that trigger a warning message.</td>
</tr>
<tr>
<td></td>
<td>• routes—The first number represents the maximum number of routes. The second number represents the number of routes that trigger a warning message.</td>
</tr>
<tr>
<td>Direct</td>
<td>Routes on the directly connected network.</td>
</tr>
<tr>
<td>Local</td>
<td>Local routes.</td>
</tr>
<tr>
<td>protocol-name</td>
<td>Name of the protocol from which the route was learned. For example, OSPF, RSVP, and Static.</td>
</tr>
</tbody>
</table>
Sample Output

show route summary

user@host> show route summary

Autonomous system number: 69
Router ID: 10.255.71.52
Maximum-ECMP: 32
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
  Restart Complete
    Direct: 6 routes, 5 active
    Local: 4 routes, 4 active
    OSPF: 5 routes, 4 active
    Static: 7 routes, 7 active
    IGMP: 1 routes, 1 active
    PIM: 2 routes, 2 active

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete
    RSVP: 2 routes, 2 active

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Restart Complete
    Direct: 1 routes, 1 active

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
  Restart Complete
    MPLS: 3 routes, 3 active
    VPLS: 4 routes, 2 active

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  Restart Complete
    Direct: 2 routes, 2 active
    PIM: 2 routes, 2 active
    MLD: 1 routes, 1 active

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
    BGP: 2 routes, 2 active
    L2VPN: 2 routes, 2 active

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
  Restart Complete
    BGP: 2 routes, 2 active
    L2VPN: 1 routes, 1 active

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
    BGP: 4 routes, 4 active

show route summary table

user@host> show route summary table inet

Router ID: 192.168.0.1
inet.0: 32 destinations, 34 routes (31 active, 0 holddown, 1 hidden)
  Direct: 6 routes, 5 active
  Local: 9 routes, 9 active
OSPF: 3 routes, 1 active
Static: 13 routes, 13 active
IGMP: 1 route, 1 active
PIM: 2 routes, 2 active

inet.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Multicast: 1 routes, 1 active

inet6.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
  Local: 1 route, 1 active
  PIM: 2 routes, 2 active

inet6.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Multicast: 1 route, 1 active

show route summary table (with Route Limits Configured for the Routing Table)

user@host> show route summary table VPN-A.inet.0

Autonomous system number: 100
Router ID: 10.255.182.142

VPN-A.inet.0: 13 destinations, 14 routes (13 active, 0 holddown, 0 hidden)
Limit/Threshold: 2000/200 destinations 20/12 routes
  Direct: 2 routes, 2 active
  Local: 1 route, 1 active
  OSPF: 4 routes, 3 active
  BGP: 4 routes, 4 active
  IGMP: 1 route, 1 active
  PIM: 2 routes, 2 active
show route table

List of Syntax
Syntax (EX Series Switches, QFX Series Switches) on page 2466

Syntax
show route table routing-table-name
   <brief | detail | extensive | terse>
   <logical-system (all | logical-system-name)>

Syntax (EX Series Switches, QFX Series Switches)
show route table routing-table-name
   <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.
Show route table evpn statement introduced in Junos OS Release 15.1X53-D30 for QFX Series switches.

Description
Display the route entries in a particular routing table.

Options
brief | detail | extensive | terse—(Optional) Display the specified level of output.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

routing-table-name—Display route entries for all routing tables whose names begin with this string (for example, inet.0 and inet6.0 are both displayed when you run the show route table inet command).

Required Privilege
view

Related Documentation
• show route summary on page 2462

List of Sample Output
show route table bgp.l2vpn.0 on page 2478
show route table bgp.l3vpn.0 on page 2478
show route table bgp.l3vpn.0 detail on page 2478
show route table bgp.rtarget.0 (When Proxy BGP Route Target Filtering Is Configured) on page 2480
show route table bgp.evpn.0 on page 2480
show route table evpna.evpn.0 on page 2481
show route table inet.0 on page 2481
show route table inet.3 on page 2481
show route table inet.3 protocol ospf on page 2481
show route table inet6.0 on page 2482
show route table inet6.3 on page 2482
show route table inetflow detail on page 2482
show route table inetflow.0 extensive (BGP Flowspec Redirect to IP) on page 2483
show route table lsdist.0 extensive on page 2484
show route table l2circuit.0 on page 2486
show route table lsdist.0 on page 2486
show route table mpls on page 2487
show route table mpls extensive on page 2487
show route table mpls.0 on page 2487
show route table mpls.0 detail (PTX Series) on page 2488
show route table mpls.0 ccc ge-0/0/1.1004 detail on page 2489
show route table mpls.0 protocol evpn on page 2490
show route table mpls.0 protocol ospf on page 2496
show route table mpls.0 extensive (PTX Series) on page 2496
show route table mpls.0 (RSVP Route—Transit LSP) on page 2497
show route table vpls_1 detail on page 2497
show route table vpn-a on page 2498
show route table vpn-a.mdt.0 on page 2498
show route table VPN-A detail on page 2498
show route table VPN-AB.inet.0 on page 2499
show route table VPN_blue.mvpn-inet6.0 on page 2499
show route table vrf1.mvpn.0 extensive on page 2500
show route table inetflow detail on page 2500
show route table bgp.evpn.0 extensive | no-more (EVPN) on page 2503
show route table default-switch.evpn.0 extensive on page 2507
show route table evpn1.evpn-mcs on page 2507
show route table evpn1 (Multihomed Proxy MAC and IP Address) on page 2507

Output Fields  Table 168 on page 2252 describes the output fields for the show route table command. Output fields are listed in the approximate order in which they appear.

Table 187: show route table 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>
</tbody>
</table>
### Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart complete</td>
<td>All protocols have restarted for this routing table.</td>
</tr>
<tr>
<td></td>
<td><strong>Restart state:</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending:</strong> <em>protocol-name</em>—List of protocols that have not yet completed graceful restart for this routing table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong>—All protocols have restarted for this routing table.</td>
</tr>
<tr>
<td></td>
<td>For example, if the output shows-</td>
</tr>
<tr>
<td>LDP.inet.0</td>
<td>: 5 routes (4 active, 1 holddown, 0 hidden)</td>
</tr>
<tr>
<td></td>
<td>Restart Pending: OSPF LDP VPN</td>
</tr>
<tr>
<td></td>
<td>This indicates that OSPF, LDP, and VPN protocols did not restart for the LDP.inet.0 routing table.</td>
</tr>
<tr>
<td>vpls_1.l2vpn.0</td>
<td>: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)</td>
</tr>
<tr>
<td></td>
<td>Restart Complete</td>
</tr>
<tr>
<td></td>
<td>This indicates that all protocols have restarted for the vpls_1.l2vpn.0 routing table.</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active)</td>
</tr>
<tr>
<td></td>
<td>• holddown (routes that are in the pending state before being declared inactive)</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
</tr>
</tbody>
</table>
Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>route-destination</strong></td>
<td>Route destination (for example: 10.0.0.1/24). The <em>entry</em> value is the number of routes for this destination, and the <em>announced</em> value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td>• <strong>MPLS-label</strong> (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• <strong>interface-name</strong> (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address;control-word-status;encapsulation type;vc-id;source</strong> (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1::Local/96).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address</strong>—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>control-word-status</strong>—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord.</td>
</tr>
<tr>
<td></td>
<td>• <strong>encapsulation type</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vc-id</strong>—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>• <strong>source</strong>—Source of the advertisement: Local or Remote.</td>
</tr>
<tr>
<td></td>
<td>• <strong>inclusive multicast Ethernet tag route</strong>—Type of route destination represented by (for example, 3:100.100.100.10:100::0::100.100.100.10/384):</td>
</tr>
<tr>
<td></td>
<td>• <strong>route distinguisher</strong>—(8 octets) Route distinguisher (RD) must be the RD of the EVPN instance (EVI) that is advertising the NLRI.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ethernet tag ID</strong>—(4 octets) Identifier of the Ethernet tag. Can set to 0 or to a valid Ethernet tag value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP address length</strong>—(1 octet) Length of IP address in bits.</td>
</tr>
<tr>
<td></td>
<td>• <strong>originating router's IP address</strong>—(4 or 16 octets) Must set to the provider edge (PE) device's IP address. This address should be common for all EVIs on the PE device, and may be the PE device's loopback address.</td>
</tr>
<tr>
<td><strong>label stacking</strong></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>S=0 route</strong> indicates that a packet with an incoming label stack depth of 2 or more exits this routing device with one fewer label (the label-popping operation is performed).</td>
</tr>
<tr>
<td></td>
<td>• If there is no <strong>S=</strong> information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).</td>
</tr>
<tr>
<td><strong>[protocol, preference]</strong></td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• *—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.</td>
</tr>
</tbody>
</table>

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.
Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>(IS-IS only). In IS-IS, a single 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.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>IP subnet augmented with a 64-bit prefix.</td>
</tr>
<tr>
<td>PMSI</td>
<td>Provider multicast service interface (MVPN routing table).</td>
</tr>
<tr>
<td>Next-hop type</td>
<td>Type of next hop. For a description of possible values for this field, see Table 172 on page 2310.</td>
</tr>
<tr>
<td>Next-hop reference count</td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td>Flood next hop 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>
<tr>
<td>via</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Label-switched-path lsp-path-name</td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td>Label operation</td>
<td>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).</td>
</tr>
<tr>
<td>Interface</td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td>Protocol next hop</td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to derive a forwarding next hop.</td>
</tr>
<tr>
<td>Indirect next hop</td>
<td>Index designation used to specify the mapping between protocol next hops, tags, kernel export policy, and the forwarding next hops.</td>
</tr>
<tr>
<td>State</td>
<td>State of the route (a route can be in more than one state). See Table 173 on page 2312.</td>
</tr>
</tbody>
</table>
### Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local AS</td>
<td>AS number of the local routing devices.</td>
</tr>
<tr>
<td>Age</td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td>AIGP</td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
<tr>
<td>Metricn</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>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>The number of BGP peers or protocols to which Junos OS has announced this route, followed by the list of the recipients of the announcement. Junos OS can also announce the route to the kernel routing table (KRT) for installing the route into the Packet Forwarding Engine, to a resolve tree, a Layer 2 VC, or even a VPN. For example, n-Resolve inet indicates that the specified route is used for route resolution for next hops found in the routing table.</td>
</tr>
<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>
</tbody>
</table>

When AS path numbers are included in the route, the format is as follows:

- [ ]—Brackets enclose the number that precedes the AS path. This number represents the number of ASs present in the AS path, when calculated as defined in RFC 4271. This value is used in the AS-path merge process, as defined in RFC 4893.
- [ ]—If more than one AS number is configured on the routing device, or if AS path prepending is configured, brackets enclose the local AS number associated with the AS path.
- { }—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.
- ()—Parentheses enclose a confederation.
- ( [ ] )—Parentheses and brackets enclose a confederation set.

**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.
### Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>validation-state</td>
<td>(BGP-learned routes) Validation status of the route:</td>
</tr>
<tr>
<td>• Invalid</td>
<td>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>• Unknown</td>
<td>Indicates that the prefix is not among the prefixes or prefix ranges in the database.</td>
</tr>
<tr>
<td>• Unverified</td>
<td>Indicates that the origin of the prefix is not verified against the database. This is because the database got populated and the validation is not called for in the BGP import policy, although origin validation is enabled, or the origin validation is not enabled for the BGP peers.</td>
</tr>
<tr>
<td>• Valid</td>
<td>Indicates that the prefix and autonomous system pair are found in the database.</td>
</tr>
<tr>
<td>FECs bound to route</td>
<td>Indicates 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>Primary Upstream</td>
<td>When multipoint LDP with multicast-only fast route (MoFRR) is configured, indicates 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, indicates 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>Prefixes bound to route</td>
<td>Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See Table 174 on page 2314 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>
</tbody>
</table>
Table 187: show route table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accepted Multipath</td>
<td>Current active path when BGP multipath is configured.</td>
</tr>
<tr>
<td>Accepted LongLivedStale</td>
<td>The LongLivedStale flag indicates that the route was marked LLGR-stale by this router, as part of the operation of LLGR receiver mode. Either this flag or the LongLivedStaleImport flag might be displayed for a route. Neither of these flags is displayed at the same time as the Stale (ordinary GR stale) flag.</td>
</tr>
<tr>
<td>Accepted LongLivedStaleImport</td>
<td>The LongLivedStaleImport flag indicates that the route was marked LLGR-stale when it was received from a peer, or by import policy. Either this flag or the LongLivedStale flag might be displayed for a route. Neither of these flags is displayed at the same time as the Stale (ordinary GR stale) flag. Accept all received BGP long-lived graceful restart (LLGR) and LLGR stale routes learned from configured neighbors and import into the inet.0 routing table.</td>
</tr>
<tr>
<td>ImportAccepted LongLivedStaleImport</td>
<td>Accept all received BGP long-lived graceful restart (LLGR) and LLGR stale routes learned from configured neighbors and imported into the inet.0 routing table. The LongLivedStaleImport flag indicates that the route was marked LLGR-stale when it was received from a peer, or by import policy.</td>
</tr>
<tr>
<td>Accepted Multipath Contrib</td>
<td>Path currently contributing to BGP multipath.</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 Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</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>
</tbody>
</table>

Table 172 on page 2310 describes all possible values for the Next-hop Types output field.

Table 188: Next-hop Types Output Field Values

<table>
<thead>
<tr>
<th>Next-Hop Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast (bcast)</td>
<td>Broadcast next hop.</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny next hop.</td>
</tr>
<tr>
<td>Discard</td>
<td>Discard next hop.</td>
</tr>
<tr>
<td>Flood</td>
<td>Flood next hop. Consists of components called branches, up to a maximum of 32 branches. Each flood next-hop branch sends a copy of the traffic to the forwarding interface. Used by point-to-multipoint RSVP, point-to-multipoint LDP, point-to-multipoint CCC, and multicast.</td>
</tr>
<tr>
<td>Next-Hop Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hold</td>
<td>Next hop is waiting to be resolved into a unicast or multicast type.</td>
</tr>
<tr>
<td>Indexed (idxd)</td>
<td>Indexed next hop.</td>
</tr>
<tr>
<td>Indirect (indr)</td>
<td>Used with applications that have a protocol next hop address that is remote. You are likely to see this next-hop type for internal BGP (IBGP) routes when the BGP next hop is a BGP neighbor that is not directly connected.</td>
</tr>
<tr>
<td>Interface</td>
<td>Used for a network address assigned to an interface. Unlike the router next hop, the interface next hop does not reference any specific node on the network.</td>
</tr>
<tr>
<td>Local (locl)</td>
<td>Local address on an interface. This next-hop type causes packets with this destination address to be received locally.</td>
</tr>
<tr>
<td>Multicast (mcst)</td>
<td>Wire multicast next hop (limited to the LAN).</td>
</tr>
<tr>
<td>Multicast discard (mdsc)</td>
<td>Multicast discard.</td>
</tr>
<tr>
<td>Multicast group (mgrp)</td>
<td>Multicast group member.</td>
</tr>
<tr>
<td>Receive (recv)</td>
<td>Receive.</td>
</tr>
<tr>
<td>Reject (rjct)</td>
<td>Discard. An ICMP unreachable message was sent.</td>
</tr>
<tr>
<td>Resolve (rslv)</td>
<td>Resolving next hop.</td>
</tr>
<tr>
<td>Routed multicast (mcrt)</td>
<td>Regular multicast next hop.</td>
</tr>
<tr>
<td>Router</td>
<td>A specific node or set of nodes to which the routing device forwards packets that match the route prefix.</td>
</tr>
<tr>
<td></td>
<td>To qualify as a next-hop type router, the route must meet the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• Must not be a direct or local subnet for the routing device.</td>
</tr>
<tr>
<td></td>
<td>• Must have a next hop that is directly connected to the routing device.</td>
</tr>
<tr>
<td>Table</td>
<td>Routing table next hop.</td>
</tr>
<tr>
<td>Unicast (ucst)</td>
<td>Unicast.</td>
</tr>
<tr>
<td>Unilist (ulst)</td>
<td>List of unicast next hops. A packet sent to this next hop goes to any next hop in the list.</td>
</tr>
</tbody>
</table>
Table 173 on page 2312 describes all possible values for the State output field. A route can be in more than one state (for example, `<Active NoReadvrt Int Ext>`).

**Table 189: State Output Field Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Route needs accounting.</td>
</tr>
<tr>
<td>Active</td>
<td>Route is active.</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>Clone</td>
<td>Route is a clone.</td>
</tr>
<tr>
<td>Cluster list length</td>
<td>Length of cluster list sent by the route reflector.</td>
</tr>
<tr>
<td>Delete</td>
<td>Route has been deleted.</td>
</tr>
<tr>
<td>Ex</td>
<td>Exterior route.</td>
</tr>
<tr>
<td>Ext</td>
<td>BGP route received from an external BGP neighbor.</td>
</tr>
<tr>
<td>FlashAll</td>
<td>Forces all protocols to be notified of a change to any route, active or inactive, for a prefix. When not set, protocols are informed of a prefix only when the active route changes.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Route not used because of routing policy.</td>
</tr>
<tr>
<td>IfCheck</td>
<td>Route needs forwarding RPF check.</td>
</tr>
<tr>
<td>IGP metric</td>
<td>Path through next hop with lower IGP metric is available.</td>
</tr>
<tr>
<td>Inactive reason</td>
<td>Flags for this route, which was not selected as best for a particular destination.</td>
</tr>
<tr>
<td>Initial</td>
<td>Route being added.</td>
</tr>
<tr>
<td>Int</td>
<td>Interior route.</td>
</tr>
<tr>
<td>Int Ext</td>
<td>BGP route received from an internal BGP peer or a BGP confederation peer.</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>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Preference</td>
<td>Path with a higher local preference value is available.</td>
</tr>
<tr>
<td>Martian</td>
<td>Route is a martian (ignored because it is obviously invalid).</td>
</tr>
<tr>
<td>MartianOK</td>
<td>Route exempt from martian filtering.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Path with lower metric next hop is available.</td>
</tr>
<tr>
<td>No difference</td>
<td>Path from neighbor with lower IP address is available.</td>
</tr>
<tr>
<td>NoReadvrt</td>
<td>Route not to be advertised.</td>
</tr>
<tr>
<td>NotBest</td>
<td>Route not chosen because it does not have the lowest MED.</td>
</tr>
<tr>
<td>Not Best in its group</td>
<td>Incoming BGP AS is not the best of a group (only one AS can be the best).</td>
</tr>
<tr>
<td>NotInstall</td>
<td>Route not to be installed in the forwarding table.</td>
</tr>
<tr>
<td>Number of gateways</td>
<td>Path with a greater 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>Pending</td>
<td>Route pending because of a hold-down configured on another route.</td>
</tr>
<tr>
<td>Release</td>
<td>Route scheduled for release.</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 lower preference value is available.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Path through a neighbor with lower ID is available.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Route not a primary route.</td>
</tr>
<tr>
<td>Unusable path</td>
<td>Path is not usable because of one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• The route is damped.</td>
</tr>
<tr>
<td></td>
<td>• The route is rejected by an import policy.</td>
</tr>
<tr>
<td></td>
<td>• The route is unresolved.</td>
</tr>
<tr>
<td>Update source</td>
<td>Last tiebreaker is the lowest IP address value.</td>
</tr>
</tbody>
</table>
Table 174 on page 2314 describes the possible values for the Communities output field.

### Table 190: Communities Output Field Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-number</td>
<td>4 bytes, encoding a 32-bit area number. For AS-external routes, the value is 0. A nonzero value identifies the route as internal to the OSPF domain, and as within the identified area. Area numbers are relative to a particular OSPF domain.</td>
</tr>
<tr>
<td>bandwidth: local AS number: link-bandwidth-number</td>
<td>Link-bandwidth community value used for unequal-cost load balancing. When BGP has several candidate paths available for multipath purposes, it does not perform unequal-cost load balancing according to the link-bandwidth community unless all candidate paths have this attribute.</td>
</tr>
<tr>
<td>domain-id</td>
<td>Unique configurable number that identifies the OSPF domain.</td>
</tr>
<tr>
<td>domain-id-vendor</td>
<td>Unique configurable number that further identifies the OSPF domain.</td>
</tr>
<tr>
<td>link-bandwidth-number</td>
<td>Link-bandwidth number: from 0 through 4,294,967,295 (bytes per second).</td>
</tr>
<tr>
<td>local AS number</td>
<td>Local AS number: from 1 through 65,535.</td>
</tr>
<tr>
<td>options</td>
<td>1 byte. Currently this is only used if the route type is 5 or 7. Setting the least significant bit in the field indicates that the route carries a type 2 metric.</td>
</tr>
<tr>
<td>origin</td>
<td>(Used with VPNs) Identifies where the route came from.</td>
</tr>
<tr>
<td>ospf-route-type</td>
<td>1 byte, encoded as 1 or 2 for intra-area routes (depending on whether the route came from a type 1 or a type 2 LSA); 3 for summary routes; 5 for external routes (area number must be 0); 7 for NSSA routes; or 129 for sham link endpoint addresses.</td>
</tr>
<tr>
<td>route-type-vendor</td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x8000. The format is area-number:ospf-route-type:options.</td>
</tr>
<tr>
<td>rte-type</td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x0306. The format is area-number:ospf-route-type:options.</td>
</tr>
<tr>
<td>target</td>
<td>Defines which VPN the route participates in; target has the format 32-bit IP address:16-bit number. For example, 10.19.0.0:100.</td>
</tr>
<tr>
<td>unknown IANA</td>
<td>Incoming IANA codes with a value between 0x1 and 0x7fff. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
<tr>
<td>unknown OSPF vendor community</td>
<td>Incoming IANA codes with a value above 0x8000. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
<tr>
<td>evpn-mcast-flags</td>
<td>Identifies the value in the multicast flags extended community and whether snooping is enabled. A value of 0x1 indicates that the route supports IGMP proxy.</td>
</tr>
</tbody>
</table>
Table 190: Communities Output Field Values (continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>evpn-l2-info</td>
<td>Identifies whether Multihomed Proxy MAC and IP Address Route Advertisement is enabled. A value of 0x20 indicates that the proxy bit is set. Use the show bridge mac-ip-table extensive statement to determine whether the MAC and IP address route was learned locally or from a PE device.</td>
</tr>
</tbody>
</table>

Sample Output

**show route table bgp.l2vpn.0**

```
user@host> show route table bgp.l2vpn.0

bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

  *[BGP/170] 01:08:58, localpref 100, from 192.168.24.1
  AS path: I
  > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am
```

**show route table bgp.l3vpn.0**

```
user@host> show route table bgp.l3vpn.0

bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.71.15:100:10.255.71.17/32
  *[BGP/170] 00:03:59, MED 1, localpref 100, from 10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100020, Push 100011(top)
10.255.71.15:200:10.255.71.18/32
  *[BGP/170] 00:03:59, MED 1, localpref 100, from 10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100021, Push 100011(top)
```

**show route table bgp.l3vpn.0 detail**

```
user@host> show route table bgp.l3vpn.0 detail

bgp.l3vpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)

10.255.245.12:1:172.16.4.0/8 (1 entry, 1 announced)
  *BGP Preference: 170/-101
  Route Distinguisher: 10.255.245.12:1
  Source: 10.255.245.12
  Next hop: 192.168.208.66 via fe-0/0/0.0, label-switched-path am
  Label operation: Push 182449
  Protocol next hop: 10.255.245.12
  Push 182449
  Indirect next hop: 863a630 297
  State: <Active Int Ext>
```
<table>
<thead>
<tr>
<th>Local AS:</th>
<th>35</th>
<th>Peer AS:</th>
<th>35</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age:</td>
<td>12:19</td>
<td>Metric2:</td>
<td>1</td>
</tr>
<tr>
<td>Task:</td>
<td>BGP_35.10.255.245.12+179</td>
<td>Announcement bits (1):</td>
<td>0-BGP.0.0.0.0+179</td>
</tr>
<tr>
<td>AS path:</td>
<td>30 10458 14203 2914 3356 I (Atomic) Aggregator: 3356 4.68.0.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communities:</td>
<td>2914:420 target:11111:1 origin:56:78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Label:</td>
<td>182449</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Localpref:</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router ID:</td>
<td>10.255.245.12</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.255.245.12:1:4.17.225.0/24 (1 entry, 1 announced)

*BGP
| Preference:       | 170/-101    |
| Route Distinguisher: | 10.255.245.12:1 |
| Source:           | 10.255.245.12 |
| Next hop:         | 192.168.208.66 via fe-0/0/0.0, selected |
| Label operation:  | Push 182465  |
| Protocol next hop:| 10.255.245.12 |
| Push 182465       |
| Indirect next hop:| 863a8f0 305  |
| State:            | <Active Int Ext> |
| Local AS:         | 35 Peer AS: | 35 |
| Age:              | 12:19       | Metric2:         | 1           |
| Task:             | BGP_35.10.255.245.12+179 | Announcement bits (1): | 0-BGP.0.0.0.0+179 |
| AS path:          | 30 10458 14203 2914 11853 11853 6496 6496 6496 6496 6496 6496 6496 I |
| Communities:      | 2914:410 target:12:34 target:11111:1 origin:12:34 |
| VPN Label:        | 182465      |
| Localpref:        | 100         |
| Router ID:        | 10.255.245.12 |

10.255.245.12:1:4.17.226.0/23 (1 entry, 1 announced)

*BGP
| Preference:       | 170/-101    |
| Route Distinguisher: | 10.255.245.12:1 |
| Source:           | 10.255.245.12 |
| Next hop:         | 192.168.208.66 via fe-0/0/0.0, selected |
| Label operation:  | Push 182465  |
| Protocol next hop:| 10.255.245.12 |
| Push 182465       |
| Indirect next hop:| 86bd210 330  |
| State:            | <Active Int Ext> |
| Local AS:         | 35 Peer AS: | 35 |
| Age:              | 12:19       | Metric2:         | 1           |
| Task:             | BGP_35.10.255.245.12+179 | Announcement bits (1): | 0-BGP.0.0.0.0+179 |
| AS path:          | 30 10458 14203 2914 11853 11853 6496 6496 6496 6496 6496 6496 6496 I |
| Communities:      | 2914:410 target:12:34 target:11111:1 origin:12:34 |
| VPN Label:        | 182465      |
| Localpref:        | 100         |
| Router ID:        | 10.255.245.12 |

10.255.245.12:1:4.17.251.0/24 (1 entry, 1 announced)

*BGP
| Preference:       | 170/-101    |
| Route Distinguisher: | 10.255.245.12:1 |
| Source:           | 10.255.245.12 |
| Next hop:         | 192.168.208.66 via fe-0/0/0.0, selected |
| Label operation:  | Push 182465  |
| Protocol next hop:| 10.255.245.12 |

Copyright © 2019, Juniper Networks, Inc.
Push 182465
Indirect next hop: 86bd210 330
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP.35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100

show route table bgp.rtarget.0 (When Proxy BGP Route Target Filtering Is Configured)

user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
100:100:100/96
  *[RTarget/5] 00:03:14
    Type Proxy
    for 10.255.165.103
    for 10.255.166.124
    Local

show route table bgp.evpn.0

user@host> show route table bgp.evpn.0
bgp.evpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
2:100.100.100.2:100::0::00:26:88:5f:67:b0/304
  *[BGP/170] 11:00:05, localpref 100, from 100.100.100.2
  AS path: I, validation-state: unverified
  > to 100.64.12.2 via xe-2/2/0.0, label-switched-path R0toR1
2:100.100.100.2:100::0::00:51:51:51:51:51/304
  *[BGP/170] 11:00:05, localpref 100, from 100.100.100.2
  AS path: I, validation-state: unverified
  > to 100.64.12.2 via xe-2/2/0.0, label-switched-path R0toR1
2:100.100.100.3:100::00:00:52:52:52:52:52/304
  *[BGP/170] 10:59:58, localpref 100, from 100.100.100.3
  AS path: I, validation-state: unverified
  > to 100.64.13.3 via ge-2/0/8.0, label-switched-path R0toR2
2:100.100.100.3:100::0::00:52:52:52:52:52/304
  *[BGP/170] 10:59:58, localpref 100, from 100.100.100.3
  AS path: I, validation-state: unverified
  > to 100.64.13.3 via ge-2/0/8.0, label-switched-path R0toR2
3:100.100.100.2:100::1000::100.100.100.2/304
  *[BGP/170] 11:00:06, localpref 100, from 100.100.100.2
  AS path: I, validation-state: unverified
  > to 100.64.12.2 via xe-2/2/0.0, label-switched-path R0toR1
3:100.100.100.2:100::2000::100.100.100.2/304
  *[BGP/170] 11:00:16, localpref 100, from 100.100.100.2
  AS path: I, validation-state: unverified
  > to 100.64.12.2 via xe-2/2/0.0, label-switched-path R0toR1
show route table evpna.evpn.0

user@host> show route table evpna.evpn.0

evpna.evpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3:100.100.100.10:100::0::10::100.100.100.10/384
   *[EVPN/170] 01:37:09
   Indirect

3:100.100.100.2:100::2000::100.100.100.2/304
   *[EVPN/170] 01:37:12
   Indirect

show route table inet.0

user@host> show route table inet.0

inet.0: 12 destinations, 12 routes (11 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 00:51:57
  > to 172.16.5.254 via fxp0.0

10.0.0.1/32         *[Direct/0] 00:51:58
  > via at-5/3/0.0

10.0.0.2/32         *[Local/0] 00:51:58
  Local

10.12.12.21/32     *[Local/0] 00:51:57
  Reject

10.13.13.13/32     *[Direct/0] 00:51:58
  > via t3-5/2/1.0

10.13.13.14/32     *[Local/0] 00:51:58
  Local

10.13.13.21/32     *[Local/0] 00:51:58
  Local

10.13.13.22/32     *[Direct/0] 00:33:59
  > via t3-5/2/0.0

127.0.0.1/32        *[Direct/0] 00:51:58
  > via lo0.0

10.222.5.0/24      *[Direct/0] 00:51:58
  > via fxp0.0

10.222.5.81/32     *[Local/0] 00:51:58
  Local

show route table inet.3

user@host> show route table inet.3

inet.3: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.0.5/32        *[LDP/9] 00:25:43, metric 10, tag 200
  > to 10.2.94.2 via lt-1/2/0.49
  > to 10.2.3.2 via lt-1/2/0.23

show route table inet.3 protocol ospf

user@host> show route table inet.3 protocol ospf
### inet.3

9 destinations, 18 routes (9 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Active, * = Both

1.1.1.20/32  
[L-OSPF/10] 1d 00:00:56, metric 2  
> to 10.0.10.70 via lt-1/2/0.14, Push 800020  
to 10.0.6.60 via lt-1/2/0.12, Push 800020, Push 800030 (top)

1.1.1.30/32  
[L-OSPF/10] 1d 00:01:01, metric 3  
> to 10.0.10.70 via lt-1/2/0.14, Push 800030  
to 10.0.6.60 via lt-1/2/0.12, Push 800030

1.1.1.40/32  
[L-OSPF/10] 1d 00:01:01, metric 4  
> to 10.0.10.70 via lt-1/2/0.14, Push 800040  
to 10.0.6.60 via lt-1/2/0.12, Push 800040

1.1.1.50/32  
[L-OSPF/10] 1d 00:01:01, metric 5  
> to 10.0.10.70 via lt-1/2/0.14, Push 800050  
to 10.0.6.60 via lt-1/2/0.12, Push 800050

1.1.1.60/32  
[L-OSPF/10] 1d 00:01:01, metric 6  
> to 10.0.10.70 via lt-1/2/0.14, Push 800060  
to 10.0.6.60 via lt-1/2/0.12, Pop

### show route table inet6.0

user@host> show route table inet6.0

inet6.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Route, * = Both

fec0:0:0:3::/64 *[Direct/0] 00:01:34  
> via fe-0/1/0.0

fec0:0:0:3::/128 *[Local/0] 00:01:34  
> Local

fec0:0:0:4::/64 *[Static/5] 00:01:34  
> to fec0:0:0:3::ffff via fe-0/1/0.0

### show route table inet6.3

user@router> show route table inet6.3

inet6.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Active, * = Both

::10.255.245.195/128  
*[LDP/9] 00:00:22, metric 1  
> via so-1/0/0.0

::10.255.245.196/128  
*[LDP/9] 00:00:08, metric 1  
> via so-1/0/0.0, Push 100008

### show route table inetflow detail

user@host> show route table inetflow detail

inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)  
10.12.44.1, */48 (1 entry, 1 announced)

*BGP  
Preference: 170/101  
Next-hop reference count: 2  
State: <Active Ext>  
Local AS: 64502 Peer AS: 64500
| Age: 4 |
| Task: BGP_64500.10.12.99.5+3792 |
| Announcement bits (1): 0-Flow |
| AS path: 64500 I |
| Communities: traffic-rate:0:0 |
| Validation state: Accept, Originator: 10.12.99.5 |
| Via: 10.12.44.0/24, Active |
| Localpref: 100 |
| Router ID: 10.255.71.161 |

10.12.56.1, */48 (1 entry, 1 announced)
*Flow
*Preference: 5
Next-hop reference count: 2
State: <Active>
Local AS: 64502
Age: 6:30
Task: RT Flow
Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
AS path: I
Communities: 1:1

show route table inetflow.0 extensive (BGP Flowspec Redirect to IP)

user@host> show route table inetflow.0 extensive

inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
2.2.2.2, */term:1 (1 entry, 1 announced)
TSI:
KRT in dfwd;
Page 0 idx 0, (group ibgp type Internal) Type 1 val 0xb209500 (adv_entry)
Advertised metrics:
Nexthop: 21.1.4.5
Localpref: 100
AS path: [100] I
Communities: redirect-to-ip:21.1.4.5:0
Action(s): accept,count
*Flow Preference: 5
Next hop type: Indirect, Next hop index: 0
Address: 0xa2b931c
Next-hop reference count: 1
Next hop:
State: <Active>
Local AS: 69
Age: 2
Validation State: unverified
Task: RT Flow
Announcement bits (1): 0-Flow
AS path: I
Communities: redirect-to-ip:21.1.4.5:0

user@host> show route table inetflow.0 extensive

inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
2.2.2.2, */term:1 (1 entry, 1 announced)
TSI:
KRT in dfwd;
Page 0 idx 0, (group ibgp type Internal) Type 1 val 0xb209500 (adv_entry)
Advertised metrics:
Nexthop: 21.1.4.5
Localpref: 100
AS path: [100] I
Communities: redirect-to-nexthop
Action(s): accept,count
*Flow Preference: 5
Next hop type: Indirect, Next hop index: 0
Address: 0xa2b931c
Next-hop reference count: 1
Next hop:
State: <Active>
Local AS: 69
Age: 2
Validation State: unverified
Task: RT Flow
Announcement bits (1): 0-Flow
AS path: I
Communities: redirect-to-nexthop
regress@10.102.178.210> show route table inetflow.0 extensive
inetflow.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
4.4.4.4,*/term:1 (1 entry, 1 announced)
TSI:
KRT in dfwd;
Action(s): accept,count
*BGP Preference: 170/-101
Next hop type: Fictitious, Next hop index: 0
Address: 0xc5e3c30
Next-hop reference count: 3
Next hop: 21.1.4.5
State: <Active Int Ext>
Local AS: 100 Peer AS: 100
Age: 10
Validation State: unverified
Task: BGP_100.1.1.1.1+179
Announcement bits (1): 0-Flow
AS path: I
Communities: redirect-to-nexthop
Accepted
Localpref: 100
Router ID: 1.1.1.1

show route table lsdist.0 extensive

user@host> show route table lsdist.0 extensive

lsdist.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
NODE { AS:4170512532 BGP-LS ID:4170512532 ISO:3245.3412.3456.00 ISIS-L1:0 }/1152
(1 entry, 1 announced)
TSI:
Page 0 idx 0, (group ibgp type Internal) Type 1 val 0xa62f378 (adv_entry)
  Advertised metrics:
    Nexthop: Self
    Localpref: 100
    AS path: [4170512532] I
    Communities:
    Path NODE { AS:4170512532 BGP-LS ID:4170512532 ISO:3245.3412.3456.00 ISIS-L1:0 }
    Vector len 4, Val: 0
      *IS-IS Preference: 15
    Level: 1
    Next hop type: Fictitious, Next hop index: 0
    Address: 0x95dfc64
    Next-hop reference count: 9
    State: <Active NotInstall>
Local AS: 4170512532  
Age: 6:05  
Validation State: unverified  
Task: IS-IS  
Announcement bits (1): 0-BGP_RT_Background  
AS path: I  
IPv4 Router-ids:  
128.220.11.197  
Area membership:  
47 00 05 80 ff f8 00 00 01 08 00 01  
SPRING-Capabilities:  
- SRGB block [Start: 800000, Range: 256, Flags: 0xc0]  
SPRING-Algorithms:  
- Algo: 0  
TSI:  
Page 0 idx 0, (group ibgp type Internal) Type 1 val 0xa62f3cc (adv_entry)  
Advertised metrics:  
Nexthop: Self  
Localpref: 100  
AS path: [4170512532] I  
Communities:  
*IS-IS  
Preference: 15  
Level: 1  
Next hop type: Fictitious, Next hop index: 0  
Address: 0x95dfc64  
Next-hop reference count: 9  
State: <Active NotInstall>  
Local AS: 4170512532  
Age: 6:05  
Validation State: unverified  
Task: IS-IS  
Announcement bits (1): 0-BGP_RT_Background  
AS path: I  
Color: 32768  
Maximum bandwidth: 1000Mbps  
Reservable bandwidth: 1000Mbps  
Unreserved bandwidth by priority:  
0 1000Mbps  
1 1000Mbps  
2 1000Mbps  
3 1000Mbps  
4 1000Mbps  
5 1000Mbps  
6 1000Mbps  
7 1000Mbps  
Metric: 10  
TE Metric: 10  
LAN IPv4 Adj-SID - Label: 299776, Flags: 0x30, Weight: 0, Nbr: 10.220.1.83  
PREFIX { Node { AS:4170512532 BGP-LS ID:4170512532 ISO:3245.3412.3456.00 } { IPv4:128.220.11.197/32 } }  
ISIS-L1:0 1/1152 (1 entry, 1 announced) TSI: Page 0 idx 0, (group ibgp type Internal) Type 1 val 0xa62f43c (adv_entry)  
Advertised metrics:  
Nexthop: Self  
Localpref: 100
show route table l2circuit.0

user@host> show route table l2circuit.0

l2circuit.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.1.195:NoCtrlWord:1:1:Local/96
  *[L2CKT/7] 00:50:47
    > via so-0/1/2.0, Push 100049
    via so-0/1/3.0, Push 100049

  *[LDP/9] 00:50:14
    Discard

10.1.1.195:CtrlWord:1:2:Local/96
  *[L2CKT/7] 00:50:47
    > via so-0/1/2.0, Push 100049
    via so-0/1/3.0, Push 100049

  *[LDP/9] 00:50:14
    Discard

show route table lsdist.0

user@host> show route table lsdist.0

lsdist.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

LINK { Local { AS:4 BGP-LS ID:100 IPv4:4.4.4.4 }.{ IPv4:4.4.4.4 } Remote { AS:4 BGP-LS ID:100 IPv4:7.7.7.7 }.{ IPv4:7.7.7.7 } Undefined:0 }/1152
  *[BGP-LS-EPE/170] 00:20:56
    Fictitious

LINK { Local { AS:4 BGP-LS ID:100 IPv4:4.4.4.4 }.{ IPv4:4.4.4.4 IfIndex:339 } Remote { AS:4 BGP-LS ID:100 IPv4:7.7.7.7 }.{ IPv4:7.7.7.7 } Undefined:0 }/1152
  *[BGP-LS-EPE/170] 00:20:56
    Fictitious

LINK { Local { AS:4 BGP-LS ID:100 IPv4:4.4.4.4 }.{ IPv4:50.1.1.1 } Remote { AS:4 BGP-LS ID:100 IPv4:5.5.5.5 }.{ IPv4:50.1.1.2 } Undefined:0 }/1152
show route table mpls

```
user@host> show route table mpls
mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 00:13:55, metric 1
Receive
1                  *[MPLS/0] 00:13:55, metric 1
Receive
2                  *[MPLS/0] 00:13:55, metric 1
Receive
1024               *[VPN/0] 00:04:18
  to table red.inet.0, Pop
```

show route table mpls extensive

```
user@host> show route table mpls extensive
100000 (1 entry, 1 announced)
TSI:
KRT in-kernel 100000 /36 -> {so-1/0/0.0}
  *LDP Preference:   9
    Next hop:  via so-1/0/0.0, selected
    Pop
    State: <Active Int>
    Age: 29:50    Metric: 1
    Task: LDP
    Announcement bits (1): 0-KRT
    AS path: I
    Prefixes bound to route: 10.0.0.194/32
```

show route table mpls.0

```
user@host> show route table mpls.0
mpls.0: 18 destinations, 19 routes (18 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 11:39:56, metric 1
  to table inet.0
0(S=0)             *[MPLS/0] 11:39:56, metric 1
  to table mpls.0
1                  *[MPLS/0] 11:39:56, metric 1
Receive
2                  *[MPLS/0] 11:39:56, metric 1
  to table inet6.0
2(S=0)             *[MPLS/0] 11:39:56, metric 1
  to table mpls.0
13                 *[MPLS/0] 11:39:56, metric 1
Receive
303168             *[EVPN/7] 11:00:49, routing-instance pbbn10, route-type
  Ingress-MAC, ISID 0
    to table pbbn10.evpn-mac.0
303184             *[EVPN/7] 11:00:53, routing-instance pbbn10, route-type
```
Ingress-IM, ISID 1000
to table pbbn10.evpn-mac.0

[EVPN/7] 11:00:53, routing-instance pbbn10, route-type
Ingress-IM, ISID 2000
to table pbbn10.evpn-mac.0

303264  *[EVPN/7] 11:00:53, remote-pe 100.100.100.2, routing-instance
pbbn10, route-type
Egress-IM, ISID 1000
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303280  *[EVPN/7] 11:00:53, remote-pe 100.100.100.2, routing-instance
pbbn10, route-type
Egress-IM, ISID 2000
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303328  *[EVPN/7] 11:00:49, remote-pe 100.100.100.2, routing-instance
pbbn10, route-type
Egress-MAC, ISID 0
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303344  *[EVPN/7] 11:00:49, remote-pe 100.100.100.2, routing-instance
pbbn10, route-type
Egress-MAC, ISID 0
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303360  *[EVPN/7] 11:00:47, routing-instance pbbn10, route-type
Egress-MAC, ISID 0, BMAC 00:26:88:5f:67:b0
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303376  *[EVPN/7] 11:00:47, routing-instance pbbn10, route-type
Egress-MAC, ISID 0
> to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
303392  *[EVPN/7] 11:00:35, remote-pe 100.100.100.3, routing-instance
pbbn10, route-type
Egress-MAC, ISID 0
> to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2
303408  *[EVPN/7] 11:00:35, remote-pe 100.100.100.3, routing-instance
pbbn10, route-type
Egress-MAC, ISID 0
> to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2
303424  *[EVPN/7] 11:00:33, routing-instance pbbn10, route-type
Egress-MAC, ISID 0, BMAC a8:d0:e5:5b:01:c8
> to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2
303440  *[EVPN/7] 11:00:33, routing-instance pbbn10, route-type
Egress-MAC, ISID 0, BMAC 00:52:52:52:52:52
> to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2

show route table mpls.0 detail (PTX Series)

user@host> show route table mpls.0 detail

ge-0/0/2.600 (1 entry, 1 announced)
  *L2VPN Preference: 7
  Next hop type: Indirect
  Address: 0x9438f34
  Next-hop reference count: 2
  Next hop type: Router, Next hop index: 567
  Next hop: 10.0.0.1 via ge-0/0/1.0, selected
  Label operation: Push 299808
  Label TTL action: prop-ttl
  Load balance label: Label 299808:None;
  Session Id: 0x1
  Protocol next hop: 10.255.255.1
  Label operation: Push 299872 Offset: 252
  Label TTL action: no-prop-ttl
  Load balance label: Label 299872:Flow label PUSH;
  Composite next hop: 0x9438ed8 570 INH Session ID: 0x2
  Indirect next hop: 0x9448208 262142 INH Session ID: 0x2
  State: <Active Int>
  Age: 21         Metric2: 1
  Validation State: unverified
show route table mpls.0 ccc ge-0/0/1.1004 detail

user@host> show route table mpls.0 ccc ge-0/0/1.1004 detail

mpls.0: 121 destinations, 121 routes (121 active, 0 holddown, 0 hidden) ge-0/0/1.1004 (1 entry, 1 announced)

  EVPN Preference: 7
  Next hop type: List, Next hop index: 1048577
  Address: 0xdc14770
  Next-hop reference count: 3
  Next hop: ELNH Address 0xd011e30
    Next hop type: Indirect, Next hop index: 0
    Address: 0xd011e30
    Next-hop reference count: 3
    Protocol next hop: 100.100.100.1
    Label operation: Push 301952
    Composite next hop: 0xd011dc0 754 INH Session ID: 0x146
    Indirect next hop: 0xb69a890 1048615 INH Session ID: 0x146
      Next hop type: Router, Next hop index: 735
      Address: 0xd00e530
      Next-hop reference count: 23
      Next hop: 100.46.1.2 via ge-0/0/5.0
      Label-switched-path pe4_to_pe1
      Label operation: Push 300320
      Label TTL action: prop-ttl
      Load balance label: Label 300320: None;
      Label element ptr: 0xd00e580
      Label parent element ptr: 0x0
      Label element references: 18
      Label element child references: 16
      Label element lsp id: 5
      Next hop: ELNH Address 0xd012070
    Next hop type: Indirect, Next hop index: 0
    Address: 0xd012070
    Next-hop reference count: 3
    Protocol next hop: 100.100.100.2
    Label operation: Push 301888
    Composite next hop: 0xd012000 755 INH Session ID: 0x143
    Indirect next hop: 0xb69a9a0 1048641 INH Session ID: 0x143
      Next hop type: Router, Next hop index: 716
      Address: 0xd00e710
      Next-hop reference count: 23
      Next hop: 100.46.1.2 via ge-0/0/5.0
      Label-switched-path pe4_to_pe2
      Label operation: Push 300304
      Label TTL action: prop-ttl
      Load balance label: Label 300304: None;
      Label element ptr: 0xd00e760
      Label parent element ptr: 0x0
      Label element references: 15
      Label element child references: 13
      Label element lsp id: 6
      Next hop: ELNH Address 0xd0121f0, selected
      Next hop type: Indirect, Next hop index: 0
      Address: 0xd0121f0
      Next-hop reference count: 3
show route table mpls.0 protocol evpn

user@host> show route table mpls.0 protocol evpn

mpls.0: 121 destinations, 121 routes (121 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

  299872  *[EVPN/7] 02:30:58, routing-instance mhevpn, route-type Ingress-IM, vlan-id 10
          to table mhevpn.evpn-mac.0
  300016  *[EVPN/7] 02:30:38, routing-instance VS-1, route-type Ingress-IM, vlan-id 110
          to table VS-1.evpn-mac.0
  300032  *[EVPN/7] 02:30:38, routing-instance VS-1, route-type Ingress-IM, vlan-id 120
          to table VS-1.evpn-mac.0
  300048  *[EVPN/7] 02:30:38, routing-instance VS-1, route-type Ingress-IM, vlan-id 130
          to table VS-1.evpn-mac.0
  300064  *[EVPN/7] 02:30:38, routing-instance VS-2, route-type Ingress-IM, vlan-id 210
          to table VS-2.evpn-mac.0
  300080  *[EVPN/7] 02:30:38, routing-instance VS-2, route-type Ingress-IM, vlan-id 220
          to table VS-2.evpn-mac.0
  300096  *[EVPN/7] 02:30:38, routing-instance VS-2, route-type Ingress-IM, vlan-id 230
          to table VS-2.evpn-mac.0
          to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
  300128  *[EVPN/7] 02:29:22, routing-instance mhevpn, route-type Ingress-Aliasing
          to table mhevpn.evpn-mac.0
Ingress-Aliasing to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3

  to table VS-1.evpn-mac.0

  to table VS-2.evpn-mac.0

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-1, route-type Egress-IM, vlan-id 10
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-1, route-type Egress-IM, vlan-id 110
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-1, route-type Egress-IM, vlan-id 130
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-2, route-type Egress-IM, vlan-id 210
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-2, route-type Egress-IM, vlan-id 220
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

*([EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-2, route-type Egress-IM, vlan-id 230
  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1

  to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
   > to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
   > to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
   > to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
300480  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-1, route-type Egress-MAC
300496  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-2, route-type Egress-MAC
300560  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-1, route-type Egress-MAC
300592  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance VS-2, route-type Egress-MAC
300608  *[EVPN/7] 02:29:23, remote-pe 100.100.100.2, routing-instance vpws1004, route-type Egress, vlan-id 2004
300624  *[EVPN/7] 02:29:23, remote-pe 100.100.100.2, routing-instance vpws1010, route-type Egress, vlan-id 2010
301232  *[EVPN/7] 02:29:17, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301296  *[EVPN/7] 02:29:10, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301312  *[EVPN/7] 02:27:06, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301360  *[EVPN/7] 02:29:01, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301408  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301456  *[EVPN/7] 02:27:06, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301552  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301568  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301648  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301664  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301680  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301696  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301712  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC
301728  *[EVPN/7] 02:27:07, remote-pe 100.100.100.2, routing-instance mhevpn, route-type Egress-MAC

Copyright © 2019, Juniper Networks, Inc.
VS-1, route-type Egress-MAC
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301744  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-IM, vlan-id 230
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301760  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
vpws1010, route-type Egress, vlan-id 2010
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301776  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
mhevpn, route-type Egress-MAC
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301792  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-1, route-type Egress-IM, vlan-id 130
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301808  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
vpws1004, route-type Egress, vlan-id 2004
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301824  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
mhevpn, route-type Egress-IM, vlan-id 10
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301840  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
vpws1002, route-type Egress, vlan-id 2002
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301856  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
vpws1003, route-type Egress, vlan-id 2003
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301872  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
vpws1003, route-type Egress Protection, vlan-id 2003
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301888  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
vpws1010, route-type Egress Protection, vlan-id 1010
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301904  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-IM, vlan-id 220
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301920  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-IM, vlan-id 210
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
301936  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-IM, vlan-id 230
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301952  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
VS-2, route-type Egress-SH, vlan-id 230
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301968  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
VS-2, route-type Egress-IM, vlan-id 220
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
301984  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-SH, vlan-id 220
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302000  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
VS-2, route-type Egress-IM, vlan-id 210
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302016  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
VS-2, route-type Egress-SH, vlan-id 210
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302032  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-MAC
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302048  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
VS-2, route-type Egress-MAC
> to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302064  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302080  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302096  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
302112  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
302128  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302144  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302160  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
302176  *[EVPN/7] 02:27:07, remote-pe 100.100.100.1, routing-instance
302192  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302208  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302224  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302240  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302256  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302272  *[EVPN/7] 02:27:07, remote-pe 100.100.100.3, routing-instance
302288  *[EVPN/7] 02:27:06, remote-pe 100.100.100.1, routing-instance
302304  *[EVPN/7] 02:27:06, remote-pe 100.100.100.1, routing-instance
302320  *[EVPN/7] 02:27:06, remote-pe 100.100.100.3, routing-instance
302336  *[EVPN/7] 02:27:06, remote-pe 100.100.100.3, routing-instance
302352  *[EVPN/7] 02:27:06, remote-pe 100.100.100.3, routing-instance
302368  *[EVPN/7] 02:27:06, remote-pe 100.100.100.3, routing-instance
mhevpn, route-type Egress-IM, vlan-id 10
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302384  *[EVPN/7] 02:27:06, remote-pe 100.100.100.3, routing-instance
mhevpn, route-type Egress-SH, vlan-id 10
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302400  *[EVPN/7] 02:26:21
   via ge-0/0/1.3001, Pop
302432  *[EVPN/7] 02:26:21, remote-pe 100.100.100.3, routing-instance
vpws3001, route-type Egress, vlan-id 40000
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302448  *[EVPN/7] 02:26:21, remote-pe 100.100.100.1, routing-instance
vpws3001, route-type Egress, vlan-id 40000
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302464  *[EVPN/7] 02:26:20, remote-pe 100.100.100.2, routing-instance
vpws3001, route-type Egress, vlan-id 40000
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
302480  *[EVPN/7] 02:26:14
   via ge-0/0/1.3016, Pop
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302512  *[EVPN/7] 02:26:14, remote-pe 100.100.100.1, routing-instance
vpws3016, route-type Egress, vlan-id 40016
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302528  *[EVPN/7] 02:26:14, remote-pe 100.100.100.2, routing-instance
vpws3016, route-type Egress, vlan-id 40016
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
302560  *[EVPN/7] 02:26:06
   via ae10.3011, Pop
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302592  *[EVPN/7] 02:26:07, remote-pe 100.100.100.1, routing-instance
vpws3011, route-type Egress, vlan-id 401100
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302608  *[EVPN/7] 02:26:07, remote-pe 100.100.100.2, routing-instance
vpws3011, route-type Egress, vlan-id 401100
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
302624  *[EVPN/7] 02:26:07, remote-pe 100.100.100.3, routing-instance
vpws3011, route-type Egress Protection, vlan-id 301100
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302656  *[EVPN/7] 02:25:59
   via ae10.3006, Pop
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302688  *[EVPN/7] 02:26:00, remote-pe 100.100.100.2, routing-instance
vpws3006, route-type Egress, vlan-id 400600
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe2
302704  *[EVPN/7] 02:26:00, remote-pe 100.100.100.1, routing-instance
vpws3006, route-type Egress, vlan-id 400600
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe1
302720  *[EVPN/7] 02:25:59, remote-pe 100.100.100.3, routing-instance
vpws3006, route-type Egress, vlan-id 400600
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
302736  *[EVPN/7] 02:25:59, remote-pe 100.100.100.3, routing-instance
vpws3006, route-type Egress Protection, vlan-id 300600
to 100.46.1.2 via ge-0/0/5.0, label-switched-path pe4_to_pe3
g-e-0/0/1.1001  *[EVPN/7] 02:29:23
   via ge-0/0/1.1001
g-e-0/0/1.2001  *[EVPN/7] 02:29:23
   via ge-0/0/1.2001
g-e-0/0/1.1002  *[EVPN/7] 02:27:06
   via ge-0/0/1.1001
ae10.2003  *[EVPN/7] 02:29:10
   via ge-0/0/1.1003
g-e-0/0/1.1003  *[EVPN/7] 02:27:06
show route table mpls.0 protocol ospf

user@host> show route table mpls.0 protocol ospf
mpls.0: 29 destinations, 29 routes (29 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

299952             *[L-OSPF/10] 23:59:42, metric 0
> to 10.0.10.70 via lt-1/2/0.14, Pop
  to 10.0.6.60 via lt-1/2/0.12, Swap 800070, Push 800030(top)
299952(S=0)        *[L-OSPF/10] 23:59:42, metric 0
> to 10.0.10.70 via lt-1/2/0.14, Pop
  to 10.0.6.60 via lt-1/2/0.12, Swap 800070, Push 800030(top)
299968             *[L-OSPF/10] 23:59:48, metric 0
> to 10.0.6.60 via lt-1/2/0.12, Pop

show route table mpls.0 extensive (PTX Series)

user@host> show route table mpls.0 extensive
ge-0/0/2.600 (1 entry, 1 announced)
TSI: KRT in-kernel ge-0/0/2.600.0 /32 -> {composite(570)}
  *L2VPN Preference: 7
  Next hop type: Indirect
  Address: 0x9438f34
  Next-hop reference count: 2
  Next hop type: Router, Next hop index: 567
  Next hop: 10.0.0.1 via ge-0/0/1.0, selected
  Label operation: Push 299808
  Label TTL action: prop-ttl
show route table mpls.0 (RSVP Route—Transit LSP)

user@host> show route table mpls.0

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 00:37:31, metric 1
Receive
1                  *[MPLS/0] 00:37:31, metric 1
Receive
2                  *[MPLS/0] 00:37:31, metric 1
Receive
13                 *[MPLS/0] 00:37:31, metric 1
Receive
300352             *[RSVP/7/1] 00:08:00, metric 1
> to 10.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300352(S=0)       *[RSVP/7/1] 00:08:00, metric 1
> to 10.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300384             *[RSVP/7/2] 00:05:20, metric 1
> to 10.64.1.106 via ge-1/0/0.0, Pop
300384(S=0)       *[RSVP/7/2] 00:05:20, metric 1
> to 10.64.1.106 via ge-1/0/0.0, Pop

show route table vpls_1 detail

user@host> show route table vpls_1 detail
vpls_1.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

172.16.1.11:1000:1:1/96 (1 entry, 1 announced)
+L2VPN Preference: 170/-1
Receive table: vpls_1.12vpn.0
Next-hop reference count: 2
State: <Active Int Ext>
Age: 4:29:47 Metric2: 1
Task: vpls_1-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:Site-Down
Label-base: 800000, range: 8, status-vector: 0xFF

show route table vpn-a

user@host> show route table vpn-a

vpn-a.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.16.1:1:1:1/96
  *[VPN/7] 05:48:27
Discard
192.168.24.1:1:2:1/96
  *[BGP/170] 00:02:53, localpref 100, from 192.168.24.1
  AS path: I
  > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am
192.168.24.1:1:3:1/96
  *[BGP/170] 00:02:53, localpref 100, from 192.168.24.1
  AS path: I
  > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am

show route table vpn-a.mdt.0

user@host> show route table vpn-a.mdt.0

vpn-a.mdt.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
  *[MVPN/70] 01:23:05, metric2 1
  Indirect
  *[BGP/170] 00:57:49, localpref 100, from 10.255.14.218
  AS path: I
  > via so-0/0/0/0.0, label-switched-path r0e-to-r1
  *[BGP/170] 00:57:49, localpref 100, from 10.255.14.217
  AS path: I
  > via so-0/0/1.0, label-switched-path r0-to-r2

show route table VPN-A detail

user@host> show route table VPN-A detail

VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
10.255.179.9/32 (1 entry, 1 announced)
show route table VPN-AB.inet.0

user@host> show route table VPN-AB.inet.0

VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.0/30  *[OSPF/10] 00:07:24, metric 1
  > via so-7/3/1.0
10.39.1.4/30  *[Direct/0] 00:08:42
  > via so-5/1/0.0
10.39.1.6/32  *[Local/0] 00:08:46
  Local
10.255.71.16/32  *[Static/5] 00:07:24
  > via so-2/0/0.0
10.255.71.17/32  *[BGP/170] 00:07:24, MED 1, localpref 100, from
10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100020, Push 100011(top)
10.255.71.18/32  *[BGP/170] 00:07:24, MED 1, localpref 100, from
10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100021, Push 100011(top)
10.255.245.245/32  *[BGP/170] 00:08:35, localpref 100
  AS path: 2 I
  > to 10.39.1.5 via so-5/1/0.0
10.255.245.246/32  *[OSPF/10] 00:07:24, metric 1
  > via so-7/3/1.0

show route table VPN_blue.mvpn-inet6.0

user@host> show route table VPN_blue.mvpn-inet6.0

vpn_blue.mvpn-inet6.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
show route table vrf1.mvpn.0 extensive

user@host> show route table vrf1.mvpn.0 extensive

1:10.255.50.77:1:10.255.50.77/240 (1 entry, 1 announced)
  *MVPN   Preference: 70
  PMSI: Flags 0x0: Label 0: RSVP-TE:
Session_13[10.255.50.77:0:25624:10.255.50.77]
  Next hop type: Indirect
  Address: 0xbb2c944
  Next-hop reference count: 360
  Protocol next hop: 10.255.50.77
  Indirect next hop: 0x0 - INH Session ID: 0x0
  State: <Active Int Ext>
  Age: 53:03      Metric2: 1
  Validation State: unverified
  Task: mvpn global task
  Announcement bits (3): 0-PIM.vrf1 1-mvpn global task 2-rt-export
  AS path: I

show route table inetflow detail

user@host> show route table inetflow detail

inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.12.44.1,*/48 (1 entry, 1 announced)
  *BGP    Preference: 170/-101
  Next-hop reference count: 2
  State: <Active Ext>
  Local AS: 64502 Peer AS: 64500
  Age: 4
  Task: BGP_64500.10.12.99.5+3792
  Announcement bits (1): 0-Flow
  AS path: 64500 I
  Communities: traffic-rate:0:0
Validation state: Accept, Originator: 10.12.99.5
Via: 10.12.44.0/24, Active
Localpref: 100
Router ID: 10.255.71.161

10.12.56.1/48 (1 entry, 1 announced)
  Preference: 5
  Next-hop reference count: 2
  State: <Active>
  Local AS: 64502
  Age: 6:30
  Task: RT Flow
  Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
  AS path: I
  Communities: 1:1

user@host> show route table green.l2vpn.0 (VPLS Multihoming with FEC 129)
green.l2vpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.1.2:100:10.1.1.2/96 AD
  *[VPLS/170] 1d 03:11:03, metric2 1
  Indirect

10.1.1.4:100:10.1.1.4/96 AD
  *[BGP/170] 1d 03:11:02, localpref 100, from 10.1.1.4
  AS path: I, validation-state: unverified
  > via ge-1/2/1.5

10.1.1.2:100:1:0/96 MH
  *[VPLS/170] 1d 03:11:03, metric2 1
  Indirect

10.1.1.4:100:1:0/96 MH
  *[BGP/170] 1d 03:11:02, localpref 100, from 10.1.1.4
  AS path: I, validation-state: unverified
  > via ge-1/2/1.5

10.1.1.4:NoCtrlWord:5:100:100:10.1.1.2/176
  *[VPLS/7] 1d 03:11:02, metric2 1
  > via ge-1/2/1.5

10.1.1.4:NoCtrlWord:5:100:100:10.1.1.2/176
  *[LDP/9] 1d 03:11:02
  Discard

user@host> show route table red extensive
red.inet.0: 364481 destinations, 714087 routes (364480 active, 48448 holddown, 1 hidden)
10.0.0.0/32 (3 entries, 1 announced)
  State: <OnList CalcForwarding>
  TSI:
  KRT in-kernel 10.0.0.0/32 -> {composite(1048575)} Page 0 idx 1 Type 1 val 0x934342c

    Nexthop: Self
    AS path: [2] I
    Communities: target:2:1
    Path 10.0.0.0 from 10.3.0.0 Vector len 4. Val: 1
      @BGP
        Preference: 170/-1
        Route Distinguisher: 2:1
        Next hop type: Indirect
        Address: 0x258059e4
Next-hop reference count: 2
Source: 2.2.0.0
Next hop type: Router
Next hop: 10.1.1.1 via ge-1/1/9.0, selected
Label operation: Push 707633
Label TTL action: prop-ttl
Session Id: 0x17d8
Protocol next hop: 10.2.0.0
Push 16
Composite next hop: 0x25805988 - INH Session ID: 0x193c
Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
Local AS: 2 Peer AS: 2
Age: 23 Metric2: 35
Validation State: unverified
Task: BGP_172.16.2.0.0+34549
AS path: I
Communities: target:2:1
Import Accepted
VPN Label: 16
Localpref: 0
Router ID: 10.2.0.0
Primary Routing Table bgp.l3vpn.0
Composite next hops: 1
Protocol next hop: 10.2.0.0 Metric: 35
Push 16
Composite next hop: 0x25805988 - INH Session ID: 0x193c
Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
Indirect path forwarding next hops: 1
    Next hop type: Router
    Next hop: 10.1.1.1 via ge-1/1/9.0
    Session Id: 0x17d8
2.2.0.0/32 Originating RIB: inet.3
    Metric: 35
    Node path count: 1
    Forwarding nexthops: 1
    Nexthop: 10.1.1.1 via ge-1/1/9.0

BGP Preference: 170/-1
Route Distinguisher: 2:1
Next hop type: Indirect
Address: 0x9347028
Next-hop reference count: 3
Source: 10.3.0.0
Next hop type: Router, Next hop index: 702
Next hop: 10.1.4.2 via ge-1/0/0.0, selected
Label operation: Push 634278
Label TTL action: prop-ttl
Session Id: 0x17d9
Protocol next hop: 10.3.0.0
Push 16
Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da
State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>
Inactive reason: Not Best in its group - IGP metric
Local AS: 2 Peer AS: 2
Age: 3:34 Metric2: 70
Validation State: unverified
Task: BGP_172.16.3.0.0+32805
Announcement bits (2): 0-KRT 1-BGP_RT_Background
AS path: I
Communities: target:2:1
Import Accepted
VPN Label: 16
Localpref: 0
Router ID: 10.3.0.0
Primary Routing Table bgp.l3vpn.0
Composite next hops: 1
  Protocol next hop: 10.3.0.0 Metric: 70
  Push 16
  Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
  Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da
  Indirect path forwarding next hops: 1
    Next hop type: Router
    Next hop: 10.1.4.2 via ge-1/0/0.0
    Session Id: 0x17d9
  10.3.0.0/32 Originating RIB: inet.3
    Metric: 70
    Node path count: 1
    Forwarding nexthops: 1
    Next hop: 10.1.4.2 via ge-1/0/0.0

Multipath Preference: 255
Next hop type: Indirect
Address: 0x24afca30
Next-hop reference count: 1
Next hop type: Router
Next hop: 10.1.1.1 via ge-1/1/9.0, selected
Label operation: Push 70763
Label TTL action: prop-ttl
Session Id: 0x17d8
Next hop type: Router, Next hop index: 702
Next hop: 10.1.4.2 via ge-1/0/0.0
Label operation: Push 634278
Label TTL action: prop-ttl
Session Id: 0x17d9
Protocol next hop: 10.2.0.0
Push 16
Composite next hop: 0x25805988 - INH Session ID: 0x193c
Indirect next hop: 0x23eea900 - INH Session ID: 0x193c Weight 0x1

Protocol next hop: 10.3.0.0
Push 16
Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da Weight 0x4000

State: <ForwardingOnly Int Ext>
Inactive reason: Forwarding use only
Age: 23 Metric2: 35
Validation State: unverified
Task: RT
AS path: I
Communities: target:2:1

show route table bgp.evpn.0 extensive | no-more (EVPN)
user@host> show route table bgp.evpn.0 extensive | no-more
bgp.evpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
2:1000:10::100::00:aa:aa:aa:aa:aa:aa/304 (1 entry, 0 announced)
  *BGP  Preference: 170/-101

Copyright © 2019, Juniper Networks, Inc.
Route Distinguisher: 1000:10
Next hop type: Indirect
Address: 0x9420fd0
Next-hop reference count: 12
Source: 10.2.3.4
Protocol next hop: 10.2.3.4
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
State: Local AS: 17 Peer AS: 17 Age: 21:12 Metric2: 1 Validation State: unverified
Task: BGP_17.1.2.3.4+50756
AS path: I
Communities: target:1111:8388708 encapsulation0:0:0:3
Import Accepted
Route Label: 100
ESI: 00:00:00:00:00:00:00:00:00:00
Localpref: 100
Router ID: 10.2.3.4
Secondary Tables: default-switch.evpn.0
Indirect next hops: 1
Protocol next hop: 10.2.3.4 Metric: 1
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 10.10.10.1 via xe-0/0/1.0
Session Id: 0x2

1.2.3.4/32 Originating RIB: inet.0
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Nexthop: 10.92.78.102 via em0.0

2:1000:10::200:00:bb:bb:bb:bb:bb/304 (1 entry, 0 announced)
*BGP Preference: 170/-101
Route Distinguisher: 1000:10
Next hop type: Indirect
Address: 0x9420fd0
Next-hop reference count: 12
Source: 10.2.3.4
Protocol next hop: 10.2.3.4
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
State: Local AS: 17 Peer AS: 17 Age: 19:43 Metric2: 1 Validation State: unverified
Task: BGP_17.1.2.3.4+50756
AS path: I
Communities: target:2222:22 encapsulation0:0:0:3
Import Accepted
Route Label: 200
ESI: 00:00:00:00:00:00:00:00:00:00
Localpref: 100
Router ID: 10.2.3.4
Secondary Tables: default-switch.evpn.0
Indirect next hops: 1
Protocol next hop: 10.2.3.4 Metric: 1
Indirect next hop: 0x2 no-forward INH Session ID: 0x0
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 10.10.10.1 via xe-0/0/1.0
Session Id: 0x2

10.2.3.4/32 Originating RIB: inet.0
Metric: 1 Node path count: 1
Forwarding nexthops: 2
Next hop: 10.92.78.102 via em0.0

2:1000:10::300:00:cc:cc:cc:cc:30/304 (1 entry, 0 announced)
  *BGP   Preference: 170/-101
  Route Distinguisher: 1000:10
  Next hop type: Indirect
  Address: 0x9420fd0
  Next-hop reference count: 12
  Source: 10.2.3.4
  Protocol next hop: 10.2.3.4
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  State: Local AS:17 Peer AS:17 Age:17:21 Metric2:1 Validation State: unverified
  Task: BGP 17,1,2,3,4+50756
  AS path: I
  Communities: target:3333:33 encapsulation0:0:0:0:3
  Import Accepted
  Route Label: 300
  ESI: 00:00:00:00:00:00:00:00:00:00
  Localpref: 100
  Router ID: 10.2.3.4
  Secondary Tables: default-switch.evpn.0
  Indirect next hops: 1
  Protocol next hop: 10.2.3.4 Metric: 1
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  Indirect path forwarding next hops: 1
    Next hop type: Router
    Next hop: 10.10.10.1 via xe-0/0/1.0
    Session Id: 0x2
    10.2.3.4/32 Originating RIB: inet.0
    Metric: 1
    Node path count: 1
    Forwarding nexthops: 2
    Next hop: 10.92.78.102 via em0.0

3:1000:10::100::1.2.3.4/304 (1 entry, 0 announced)
  *BGP   Preference: 170/-101
  Route Distinguisher: 1000:10
  PMRI: Flags 0x0: Label 100: Type INGRESS-REPLICATION 1.2.3.4
  Next hop type: Indirect
  Address: 0x9420fd0
  Next-hop reference count: 12
  Source: 10.2.3.4
  Protocol next hop: 10.2.3.4
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  State: Local AS:17 Peer AS:17 Age:37:01 Metric2:1 Validation State: unverified
  Task: BGP 17.1.2.3.4+50756
  AS path: I
  Communities: target:1111:8388708 encapsulation0:0:0:0:3
  Import Accepted
  Localpref: 100
  Router ID: 10.2.3.4
  Secondary Tables: default-switch.evpn.0
  Indirect next hops: 1
  Protocol next hop: 10.2.3.4 Metric: 1
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  Indirect path forwarding next hops: 1
    Next hop type: Router
    Next hop: 10.10.10.1 via xe-0/0/1.0
    Session Id: 0x2
    10.2.3.4/32 Originating RIB: inet.0
    Metric: 1
    Node path count: 1
Forwarding nexthops: 2
Next hop: 10.92.78.102 via em0.0

3:1000:10::200::1.2.3.4/304 (1 entry, 0 announced)
  BGP Preference: 170/-101
  Route Distinguisher: 1000:10
  PMSI: Flags 0x0: Label 200: Type INGRESS-REPLICATION 1.2.3.4
  Next hop type: Indirect
  Address: 0x9420fd0
  Next-hop reference count: 12
  Source: 10.2.3.4
  Protocol next hop: 10.2.3.4
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  State: Local AS: 17 Peer AS: 17 Age:35:22 Metric2:1 Validation State:unverified Task: BGP 17.1.2.3.4+50756
  AS path:I Communities: target:3333:33 encapsulation):0:0:0:0:3

Import Accepted
  Localpref: 100
  Router ID: 10.2.3.4
  Secondary Tables: default-switch.evpn.0
  Indirect next hops: 1
    Protocol next hop: 10.2.3.4 Metric: 1
    Indirect next hop: 0x2 no-forward INH Session ID: 0x0
    Indirect path forwarding next hops: 1
      Next hop type: Router
      Next hop: 10.10.10.1 via xe-0/0/1.0
      Session Id: 0x2
    10.2.3.4/32 Originating RIB: inet.0
      Metric: 1 Node path count: 1
    Forwarding nexthops: 2
      Next hop: 10.92.78.102 via em0.0

3:1000:10::300::1.2.3.4/304 (1 entry, 0 announced)
  BGP Preference: 170/-101
  Route Distinguisher: 1000:10
  PMSI: Flags 0x0: Label 300: Type INGRESS-REPLICATION 1.2.3.4
  Next hop type: Indirect
  Address: 0x9420fd0
  Next-hop reference count: 12
  Source: 10.2.3.4
  Protocol next hop: 10.2.3.4
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  State: Local AS: 17 Peer AS: 17 Age:35:22 Metric2:1 Validation State:unverified Task: BGP 17.1.2.3.4+50756
  AS path:1 Communities: target:3333:33 encapsulation):0:0:0:0:3

Import Accepted
  Localpref:100
  Router ID: 10.2.3.4
  Secondary Tables: default-switch.evpn.0
  Indirect next hops: 1
    Protocol next hop: 10.2.3.4 Metric: 1
    Indirect next hop: 0x2 no-forward INH Session ID: 0x0
    Indirect path forwarding next hops: 1
      Next hop type: Router
      Next hop: 10.10.10.1 via xe-0/0/1.0
      Session Id: 0x2
    10.2.3.4/32 Originating RIB: inet.0
      Metric: 1 Node path count: 1
    Forwarding nexthops: 2
      Next hop: 10.92.78.102 via em0.0
show route table default-switch.evpn.0 extensive

The following shows the partial output listing for the EVPN VNI table.

user@host> show route table default-switch.evpn.0 extensive

3:1000:10::00:aa:aa:aa:aa::/304 (1 entry, 1 announced)
  ^BGP
  Preference: 170/-101
  Route Distinguisher: 10.255.0.1:00
  PMSI: Flags 0x0: Label 100: Type INGRESS-REPLICATION 1.2.3.4
  Next hop type: Indirect, Next hop index: 0
  Address: OxcebFad0
  Next-hop reference count: 26
  Source: 10.255.0.1
  Protocol next hop: 10.255.0.1
  Indirect next hop: 0x2 no-forward INH Session ID: 0x0
  State: <Secondary Active Int Ext>
  Local AS:   100 Peer AS:   100
  Age: 1:35:30    Metric2: 2
  Validation State: unverified
  Task: BGP_100.10.255.0.1
  Announcement bits (1): 0-default-switch-evpn
  AS path: I
  Communities: target:100:100 encapsulation:vxlan (0x8)
  evpn-mcast-flags:0x1:snooping-enabled
  ...

show route table evpn1.evpn-mcsn

The following shows the output listing for the multicast information used by the rpdp and mcsnooed.

user@host> show route table default-switch.evpn-mcsn.1

default-switch.evpn-mcsn.1: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

0.14,0.0,0.0/48  *[Multicast/180] 00:01:02
  to 1.1.1.1 via vtep.32770
  to 1.2.2.2 via vtep.32771
  to 1.6.6.6 via vtep.32769
  to 1.3.3.3 via vtep.32772

0.14,0.0,0.0,224.0.0.0/52*[Multicast/180] 00:01:02
  to 1.1.1.1 via vtep.32770
  to 1.2.2.2 via vtep.32771
  to 1.6.6.6 via vtep.32769
  to 1.3.3.3 via vtep.32772

0.14,0.0,0.0,225.1.1.1/80*[Multicast/180] 00:00:06
  to 1.1.1.1 via vtep.32770
  to 1.2.2.2 via vtep.32771
  to 1.6.6.6 via vtep.32769
  to 1.3.3.3 via vtep.32772

show route table evpn1 (Multihomed Proxy MAC and IP Address)

The following shows a partial output listing for an EVPN instance. This indicates when Multihomed Proxy MAC and IP Address Route Advertisement is enabled.

user@host> show route table evpn-1
2:666:11010003::1002::00:00:00:00:00:02::102.1.1.2/304 MAC/IP (1 entry, 1 announced)

TSI:
Page 0 idx 0, (group vteps type Internal) Type 1 val 0xb20eb10 (adv_entry)
  Advertised metrics:
    Nexthop: 103.1.1.1
    Localpref: 100
    AS path: [666] I
  Communities: target:666:1002 evpn-l2-info:0x20:proxy (mtu 0)
Path 2:666:11010003::1002::00:00:00:00:00:02::102.1.1.2 Vector len 4. Val: 0
  *EVPN
   Preference: 170
   Next hop type: Indirect, Next hop index: 0
   Address: 0xc3a9cf0
   Next-hop reference count: 36
   Protocol next hop: 103.1.1.1
   Indirect next hop: 0x0 - INH Session ID: 0x0
   State: <Active Int Ext>
show route terse

List of Syntax  Syntax on page 2509  
Syntax (EX Series Switches) on page 2509

Syntax  
show route terse 
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  show route terse

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

Description  Display a high-level summary of the routes in the routing table.

NOTE: For BGP routes, the show route terse command displays the local 
preference attribute and MED instead of the metric1 and metric2 values. This 
ismostly dueto historical reasons.

To display the metric1 and metric2 value of a BGP route, use the show route 
extensive command.

Options  none—Display a high-level summary of the routes in the routing table.  
logical-system (all | logical-system-name)—(Optional) Perform this operation on all 
logical systems or on a particular logical system.

Required Privilege  view

List of Sample Output  show route terse on page 2511

Output Fields  Table 191 on page 2509 describes the output fields for the show route terse command.  
Output fields are listed in the approximate order in which they appear.

Table 191: show route terse 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>
Table 191: show route terse Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active)</td>
</tr>
<tr>
<td></td>
<td>• holdown (routes that are in the pending state before being declared inactive)</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
</tr>
<tr>
<td>route key</td>
<td>Key for the state of the route:</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• *—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.</td>
</tr>
<tr>
<td>A</td>
<td>Active route. An asterisk (*) indicates this is the active route.</td>
</tr>
<tr>
<td>V</td>
<td>Validation status of the route:</td>
</tr>
<tr>
<td></td>
<td>• ?—Not evaluated. Indicates that the route was not learned through BGP.</td>
</tr>
<tr>
<td></td>
<td>• I—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>• N—Unknown. Indicates that the prefix is not among the prefixes or prefix ranges in the database.</td>
</tr>
<tr>
<td></td>
<td>• V—Valid. Indicates that the prefix and autonomous system pair are found in the database.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination of the route.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol through which the route was learned:</td>
</tr>
<tr>
<td></td>
<td>• A—Aggregate</td>
</tr>
<tr>
<td></td>
<td>• B—BGP</td>
</tr>
<tr>
<td></td>
<td>• C—CCC</td>
</tr>
<tr>
<td></td>
<td>• D—Direct</td>
</tr>
<tr>
<td></td>
<td>• G—GMPLS</td>
</tr>
<tr>
<td></td>
<td>• I—I-IS-IS</td>
</tr>
<tr>
<td></td>
<td>• L—L2CKT, L2VPN, LDP, Local</td>
</tr>
<tr>
<td></td>
<td>• K—Kernel</td>
</tr>
<tr>
<td></td>
<td>• M—MPLS, MSDP</td>
</tr>
<tr>
<td></td>
<td>• O—OSPF</td>
</tr>
<tr>
<td></td>
<td>• P—PIM</td>
</tr>
<tr>
<td></td>
<td>• R—RIP, RIPng</td>
</tr>
<tr>
<td></td>
<td>• S—Static</td>
</tr>
<tr>
<td></td>
<td>• T—Tunnel</td>
</tr>
<tr>
<td>Prf</td>
<td>Preference value of 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.</td>
</tr>
</tbody>
</table>
Table 191: show route terse Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric 1</td>
<td>First metric value in the route. For routes learned from BGP, this is the MED metric.</td>
</tr>
<tr>
<td>Metric 2</td>
<td>Second metric value in the route. For routes learned from BGP, this is the IGP metric.</td>
</tr>
<tr>
<td>Next hop</td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route.</td>
</tr>
</tbody>
</table>
| AS path    | 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:  
• I—IGP.  
• E—EGP.  
• ?—Incomplete; typically, the AS path was aggregated. |

Sample Output

show route terse

user@host> show route terse

inet.0: 10 destinations, 12 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A V Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* ? 172.16.1.1/32</td>
<td>O 10</td>
<td>100</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>? unverified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 172.16.1.1/32</td>
<td>B 170</td>
<td>110</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>200 I</td>
</tr>
<tr>
<td>+ V 2.2.0.2/32</td>
<td></td>
<td></td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 10.0.0.0/30</td>
<td>D 0</td>
<td>100</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>? unverified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 10.0.0.1/32</td>
<td>L 0</td>
<td>100</td>
<td></td>
<td>10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>? unverified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 10.0.0.4/30</td>
<td>B 170</td>
<td>100</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>unverified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 10.0.0.8/30</td>
<td>B 170</td>
<td>100</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>I</td>
</tr>
<tr>
<td>unverified</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ I 172.16.1.1/32</td>
<td>B 170</td>
<td>90</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>200 I</td>
</tr>
<tr>
<td>invalid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* N 192.168.2.3/32</td>
<td>B 170</td>
<td>100</td>
<td></td>
<td>&gt;10.0.0.2</td>
<td>200 I</td>
</tr>
<tr>
<td>unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* ? 172.16.233.5/32</td>
<td>O 10</td>
<td>1</td>
<td></td>
<td>MultiRecv</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
CHAPTER 26

RIP Operational Commands

- clear rip general-statistics
- clear rip statistics
- show rip general-statistics
- show rip neighbor
- show rip statistics
clear rip general-statistics

List of Syntax  Syntax on page 2514
  Syntax (EX Series Switches and QFX Series) on page 2514

Syntax  clear rip general-statistics
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)  clear rip general-statistics

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 12.1 for the QFX Series.
  Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Clear RIP general statistics.

Options  none—Clear RIP general statistics.

  logical-system (all | logical-system-name)—(Optional) Perform this operation on all
  logical systems or on a particular logical system.

Required Privilege  clear

Related Documentation  •  show rip general-statistics on page 2517

List of Sample Output  clear rip general-statistics on page 2514

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

  clear rip general-statistics

  user@host> clear rip general-statistics
clear rip statistics

List of Syntax  Syntax on page 2515  
Syntax (EX Series Switches and QFX Series) on page 2515

Syntax  clear rip statistics  
<instance (all | instance-name)>
<logical-system (all | logical-system-name)>
<neighbor>
<peer (all | address)>

Syntax (EX Series Switches and QFX Series)  clear rip statistics  
<instance (all | instance-name)>
<neighbor>

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 12.1 for the QFX Series.  
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description  Clear RIP statistics.

Options  none—Reset RIP counters for all neighbors for all routing instances.  
instance (all | instance-name)—(Optional) Clear RIP statistics for all instances or for the specified routing instance only.  
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.  
neighbor—(Optional) Clear RIP statistics for the specified neighbor only.  
peer (all | address)—(Optional) Clear RIP statistics for a single peer or all peers.

Required Privilege  clear  
Level

Related Documentation  • show rip statistics on page 2522

List of Sample Output  clear rip statistics on page 2516

Output Fields  When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear rip statistics

user@host> clear rip statistics
show rip general-statistics

List of Syntax
Syntex on page 2517
Syntex (EX Series Switches and QFX Series) on page 2517

Syntax
show rip general-statistics
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series) show rip general-statistics

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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Display brief RIP statistics.

Options
none—Display brief RIP statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

Related Documentation
• clear rip general-statistics on page 2514

List of Sample Output
show rip general-statistics on page 2518

Output Fields
Table 192 on page 2517 lists the output fields for the show rip general-statistics command. Output fields are listed in the approximate order in which they appear.

Table 192: show rip general-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad msgs</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>no recv intf</td>
<td>Number of packets received with no matching interface.</td>
</tr>
<tr>
<td>curr memory</td>
<td>Amount of memory currently used by RIP.</td>
</tr>
<tr>
<td>max memory</td>
<td>Most memory used by RIP.</td>
</tr>
</tbody>
</table>
Sample Output

show rip general-statistics

```
user@host> show rip general-statistics

RIPv2 I/O info:
bad msgs       :   0
no recv intf   :   0
curr memory   :   0
max memory     :   0
```
**show rip neighbor**

**List of Syntax**

Syntax on page 2519
Syntax (EX Series Switches and QFX Series) on page 2519

**Syntax**

`show rip neighbor`

- `<instance (all | instance-name) >`
- `<logical-system (all | logical-system-name) >`
- `<name`

**Syntax (EX Series Switches and QFX Series)**

`show rip neighbor`

- `<instance (all | instance-name) >`
- `<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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

**Description**

Display information about RIP neighbors.

**Options**

`none`—Display information about all RIP neighbors for all instances.

- `<instance (all | instance-name) >`—(Optional) Display RIP neighbor information for all instances or for only the specified routing instance.

- `<logical-system (all | logical-system-name) >`—(Optional) Perform this operation on all logical systems or on a particular logical system.

- `<name>`—(Optional) Display detailed information about only the specified RIP neighbor.

**Required Privilege Level**

`view`

**List of Sample Output**

- `show rip neighbor on page 2520`
- `show rip neighbor (With Demand Circuits Configured) on page 2520`

**Output Fields**

Table 193 on page 2520 lists the output fields for the `show rip neighbor` command. Output fields are listed in the approximate order in which they appear.
Table 193: show rip neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Name of the RIP neighbor.</td>
</tr>
</tbody>
</table>

**NOTE:** Beginning with Junos OS Release 11.1, when you configure demand circuits, the output displays a demand circuit (DC) flag next to neighbor interfaces configured for demand circuits.

If you configure demand circuits at the [edit protocols rip group group-name neighbor neighbor-name] hierarchy level, the output shows only the neighboring interface that you specifically configured as a demand circuit. If you configure demand circuits at the [edit protocols rip group group-name] hierarchy level, all of the interfaces in the group are configured as demand circuits. Therefore, the output shows all of the interfaces in that group as demand circuits.

<table>
<thead>
<tr>
<th>State</th>
<th>State of the connection: Up or Dn (Down).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Address of the port on the local router.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Address of the port on the remote router.</td>
</tr>
<tr>
<td>Send Mode</td>
<td>Send options: broadcast, multicast, none, or version 1.</td>
</tr>
<tr>
<td>Receive Mode</td>
<td>Type of packets to accept: both, none, version 1, or version 2.</td>
</tr>
<tr>
<td>In Met</td>
<td>Metric added to incoming routes when advertising into RIP routes that were learned from other protocols.</td>
</tr>
</tbody>
</table>

### Sample Output

show rip neighbor

```
user@host> show rip neighbor

Neighbor   Local  Source          Destination     Send   Receive  In  Met
--------   -----  -------         -----------     ----   -------  ---
ge-2/3/0.0  Up     192.168.9.105  192.168.9.107  bcast  both   1
at-5/1/1.42 Dn     (null)         (null)          mcast v2 only 3
at-5/1/0.42 Dn     (null)         (null)          mcast     both  3
so-0/0/0.0  Up     198.51.100.0  224.0.0.9       mcast     both  3
```

show rip neighbor (With Demand Circuits Configured)

```
user@host> show rip neighbor

Neighbor   Local  Source          Destination     Send   Receive  In  Met
--------   -----  -------         -----------     ----   -------  ---
so-0/1/0.0(DC)  Up     10.10.10.2  224.0.0.9       mcast     both  1
so-0/2/0.0(DC)  Up     192.0.2.2  224.0.0.9       mcast     both  1
```
show rip statistics

List of Syntax Syntax on page 2522
Syntax (EX Series Switches and QFX Series) on page 2522

Syntax show rip statistics
<instance (all | instance-name)>
<logical-system (all | logical-system-name)>
<name>
<peer (all | address)>

Syntax (EX Series Switches and QFX Series) show rip statistics
<instance (all | instance-name)>
<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 12.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display RIP statistics about messages sent and received on an interface, as well as information received from advertisements from other routing devices.

Options none—Display RIP statistics for all routing instances.

instance (all | instance-name)—(Optional) Display RIP statistics for all instances or for only the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

name—(Optional) Display detailed information about only the specified RIP neighbor.

peer (all | address)—(Optional) Display RIP statistics for a single peer or all peers.

Required Privilege Level view

Related Documentation • clear rip statistics on page 2515

List of Sample Output show rip statistics on page 2524

Output Fields Table 194 on page 2523 lists the output fields for the show rip statistics command. Output fields are listed in the approximate order in which they appear.
Table 194: show rip statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIP info</strong></td>
<td>Information about RIP on the specified interface:</td>
</tr>
<tr>
<td>port</td>
<td>UDP port number used for RIP.</td>
</tr>
<tr>
<td>update interval</td>
<td>Interval between routing table updates, in seconds.</td>
</tr>
<tr>
<td>holdown</td>
<td>Hold-down interval, in seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout interval, in seconds.</td>
</tr>
<tr>
<td>restart in progress</td>
<td>Graceful restart status. Displayed when RIP is or has been in the process of graceful restart.</td>
</tr>
<tr>
<td>restart time</td>
<td>Estimated time for the graceful restart to finish, in seconds.</td>
</tr>
<tr>
<td>restart will complete in</td>
<td>Remaining time for the graceful restart to finish, in seconds.</td>
</tr>
<tr>
<td>rts learned</td>
<td>Number of routes learned through RIP.</td>
</tr>
<tr>
<td>rts held down</td>
<td>Number of routes held down by RIP.</td>
</tr>
<tr>
<td>rqsts dropped</td>
<td>Number of received request packets that were dropped.</td>
</tr>
<tr>
<td>resps dropped</td>
<td>Number of received response packets that were dropped.</td>
</tr>
<tr>
<td><strong>logical-interface</strong></td>
<td>Name of the logical interface and its statistics:</td>
</tr>
<tr>
<td>routes learned</td>
<td>Number of routes learned on the logical interface.</td>
</tr>
<tr>
<td>routes advertised</td>
<td>Number of routes advertised by the logical interface.</td>
</tr>
<tr>
<td><strong>Counter</strong></td>
<td>List of counter types:</td>
</tr>
<tr>
<td>Updates Sent</td>
<td>Number of update messages sent.</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>Number of triggered update messages sent.</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>Number of response messages sent.</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>RIPv1 Updates Received</td>
<td>Number of RIPv1 update messages received.</td>
</tr>
<tr>
<td>RIPv1 Bad Route Entries</td>
<td>Number of RIPv1 invalid route entry messages received.</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored</td>
<td>Number of RIPv1 update messages ignored.</td>
</tr>
<tr>
<td>RIPv2 Updates Received</td>
<td>Number of RIPv2 update messages received.</td>
</tr>
<tr>
<td>RIPv2 Bad Route Entries</td>
<td>Number of RIPv2 invalid route entry messages received.</td>
</tr>
<tr>
<td>RIPv2 Updates Ignored</td>
<td>Number of RIPv2 update messages that were ignored.</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>Number of received update messages that failed authentication.</td>
</tr>
<tr>
<td>RIP Requests Received</td>
<td>Number of RIP request messages received.</td>
</tr>
<tr>
<td>RIP Requests Ignored</td>
<td>Number of RIP request messages ignored.</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>Total number of packets for the selected counter.</td>
</tr>
<tr>
<td><strong>Last 5 min</strong></td>
<td>Number of packets for the selected counter in the most recent 5-minute period.</td>
</tr>
<tr>
<td><strong>Last minute</strong></td>
<td>Number of packets for the selected counter in the most recent 1-minute period.</td>
</tr>
</tbody>
</table>
### Sample Output

**show rip statistics**

```
user@host> show rip statistics so-0/0/0.0

RIP info: port 520; update interval: 30s; holddown 180s; timeout 120s
restart in progress: restart time 60s; restart will complete in 55s

- rts learned | rts held down | rqsts dropped | resps dropped | Counters
- 0 | 0 | 0 | 0

so-0/0/0.0: 0 routes learned; 501 routes advertised

<table>
<thead>
<tr>
<th>Counter</th>
<th>Total</th>
<th>Last 5 min</th>
<th>Last minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
CHAPTER 27

RIPvng Operational Commands

- clear ripng general-statistics
- clear ripng statistics
- show ripng general-statistics
- show ripng neighbor
- show ripng statistics
clear ripng general-statistics

List of Syntax  Syntax on page 2526
               Syntax (EX Series Switches) on page 2526

Syntax  clear ripng general-statistics
       <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)  clear ripng general-statistics

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

Description  Clear RIP next generation (RIPng) general statistics.

Options  none—Clear RIPng general statistics.
         logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level  clear

Related Documentation  •  show ripng general-statistics on page 2528

List of Sample Output  clear ripng general-statistics on page 2526

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ripng general-statistics

          user@host> clear ripng general-statistics
clear ripng statistics

List of Syntax  Syntax on page 2527
    Syntax (EX Series Switch) on page 2527

Syntax  clear ripng statistics
        <instance | name>
        <logical-system (all | logical-system-name)>

Syntax (EX Series
Switch)  clear ripng statistics
        <instance | name>

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

Description  Clear RIP next-generation (RIPng) statistics.

Options  
        none—Reset RIPng counters for all neighbors for all routing instances.
        instance—(Optional) Reset RIPng counters for the specified instance.
        logical-system (all | logical-system-name)—(Optional) Perform this operation on all
                      logical systems or on a particular logical system.
        name—(Optional) Reset RIPng counters for the specified neighbor.

Required Privilege  clear

Related Documentation  • show ripng statistics on page 2532

List of Sample Output  clear ripng statistics on page 2527

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ripng statistics

    user@host> clear ripng statistics
show ripng general-statistics

List of Syntax  Syntax on page 2528
               Syntax (EX Series Switch) on page 2528

Syntax  show ripng general-statistics
        <logical-system (all | logical-system-name)>

Syntax (EX Series Switch)  show ripng general-statistics

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

Description  Display general RIP next-generation (RIPng) statistics.

Options  none—Display general RIPng statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all
       logical systems or on a particular logical system.

Required Privilege  view

Level

Related Documentation  •  clear ripng general-statistics on page 2526

List of Sample Output  show ripng general-statistics on page 2529

Output Fields  Table 195 on page 2528 lists the output fields for the show ripng general-statistics command.
               Output fields are listed in the approximate order in which they appear.

Table 195: show ripng general-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad msgs</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>no recv intf</td>
<td>Number of packets received with no matching interface.</td>
</tr>
<tr>
<td>curr memory</td>
<td>Amount of memory currently used by RIPng.</td>
</tr>
<tr>
<td>max memory</td>
<td>Most memory used by RIPng.</td>
</tr>
</tbody>
</table>
**Sample Output**

```plaintext
show ripng general-statistics
```

```
user@host> show ripng general-statistics

RIPng I/O info:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad msgs</td>
<td>0</td>
</tr>
<tr>
<td>no recv intf</td>
<td>0</td>
</tr>
<tr>
<td>curr memory</td>
<td>0</td>
</tr>
<tr>
<td>max memory</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Copyright © 2019, Juniper Networks, Inc.
show ripng neighbor

**List of Syntax**

Syntax on page 2530
Syntax (EX Series Switch) on page 2530

**Syntax**

```
show ripng neighbor
<logical-system (all | logical-system-name)>
<name>
```

**Syntax (EX Series Switch)**

```
show ripng neighbor
<name>
```

**Release Information**

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

**Description**

Display information about RIP next-generation (RIPv2) neighbors.

**Options**

- **none**—Display information about all RIPv2 neighbors.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **name**—(Optional) Display detailed information about a specific RIPv2 neighbor.

**Required Privilege Level**

view

**List of Sample Output**

show ripng neighbor on page 2531

**Output Fields**

Table 196 on page 2530 lists the output fields for the `show ripng neighbor` command. Output fields are listed in the approximate order in which they appear.

Table 196: `show ripng neighbor` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Name of RIPv2 neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>State of the connection: <strong>Up</strong> or <strong>Dn</strong> (Down).</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination address.</td>
</tr>
<tr>
<td>Send</td>
<td>Send options: <strong>broadcast</strong>, <strong>multicast</strong>, <strong>none</strong>, <strong>version 1</strong>, or <strong>yes</strong>.</td>
</tr>
<tr>
<td>Recv</td>
<td>Type of packets to accept: <strong>both</strong>, <strong>none</strong>, <strong>version 1</strong>, or <strong>yes</strong>.</td>
</tr>
</tbody>
</table>
### Table 196: show ripng neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In Met</strong></td>
<td>Metric added to incoming routes when advertising into RIPng routes that were learned from other protocols.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ripng neighbor**

```
user@host> show ripng neighbor

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>State</th>
<th>Source Address</th>
<th>Dest Address</th>
<th>Send</th>
<th>Recv</th>
<th>Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/2.0</td>
<td>Up</td>
<td>fe80::290:69ff:fe68:b002</td>
<td>ff02::9</td>
<td>yes</td>
<td>yes</td>
<td>1</td>
</tr>
</tbody>
</table>
```

---

Copyright © 2019, Juniper Networks, Inc.
show ripng statistics

List of Syntax  
Syntax on page 2532
Syntax (EX Series Switch) on page 2532

Syntax  
show ripng statistics
<logical-system (all | logical-system-name)>
<name>

Syntax (EX Series Switch)  
show ripng statistics
<name>

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

Description  
Display RIP next generation (RIPng) statistics about messages sent and received on an interface, as well as information received from advertisements from other routing devices.

Options  
none—Display RIPng statistics for all neighbors.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

name—(Optional) Display detailed information about a specific RIPng neighbor.

Required Privilege  
view

Related Documentation  
• clear ripng statistics on page 2527

List of Sample Output  
show ripng statistics on page 2533

Output Fields  
Table 197 on page 2533 lists the output fields for the show ripng statistics command. Output fields are listed in the approximate order in which they appear.
Table 197: show ripng statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIPng info</strong></td>
<td>Information about RIPng on the specified interface:</td>
</tr>
<tr>
<td>port</td>
<td>UDP port number used for RIPng.</td>
</tr>
<tr>
<td>holddown</td>
<td>Hold-down interval, in seconds.</td>
</tr>
<tr>
<td>rts learned</td>
<td>Number of routes learned through RIPng.</td>
</tr>
<tr>
<td>rts held down</td>
<td>Number of routes held down by RIPng.</td>
</tr>
<tr>
<td>rqsts dropped</td>
<td>Number of received request packets that were dropped.</td>
</tr>
<tr>
<td>resps dropped</td>
<td>Number of received response packets that were dropped.</td>
</tr>
<tr>
<td>restart</td>
<td>Graceful restart status. Displayed when RIPng is or has been in the process of graceful restart.</td>
</tr>
<tr>
<td><strong>logical-interface</strong></td>
<td>Name of the logical interface and its statistics:</td>
</tr>
<tr>
<td>routes learned</td>
<td>Number of routes learned on the logical interface.</td>
</tr>
<tr>
<td>routes advertised</td>
<td>Number of routes advertised by the logical interface.</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout interval, in seconds.</td>
</tr>
<tr>
<td>update interval</td>
<td>Interval between routing table updates, in seconds.</td>
</tr>
<tr>
<td><strong>Counter</strong></td>
<td>List of counter types:</td>
</tr>
<tr>
<td>Updates Sent</td>
<td>Number of update messages sent.</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>Number of triggered update messages sent.</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>Number of response messages sent.</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>Updates Received</td>
<td>Number of RIPng update messages received.</td>
</tr>
<tr>
<td>Bad Route Entries</td>
<td>Number of RIPng invalid route entry messages received.</td>
</tr>
<tr>
<td>Updates ignored</td>
<td>Number of RIPng update messages ignored.</td>
</tr>
<tr>
<td>RIPng Requests Received</td>
<td>Number of RIPng request messages received.</td>
</tr>
<tr>
<td>RIPng Requests ignored</td>
<td>Number of RIPng request messages ignored.</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>Total number of packets for the selected counter.</td>
</tr>
<tr>
<td><strong>Last 5 min</strong></td>
<td>Number of packets for the selected counter in the most recent 5-minute period.</td>
</tr>
<tr>
<td><strong>Last minute</strong></td>
<td>Number of packets for the selected counter in the most recent 1-minute period.</td>
</tr>
</tbody>
</table>

**Sample Output**

`show ripng statistics`

```
user@host> show ripng statistics
RIPng info: port 521; holddown 120s;
        rts learned 0 0 0 0
        rqsts dropped 0 0 0 0
so-0/1/3.0: 0 routes learned; 1 routes advertised; timeout 180s; update interval 20s
```

```
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th>--------</th>
<th>--------</th>
<th>--------</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates Sent</td>
<td>934</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPng Requests Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPng Requests Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
CHAPTER 28

Firewall Filter Operational Commands

- clear firewall
- show firewall
- show firewall filter version
- show firewall log
- show firewall prefix-action-stats
- show firewall templates-in-use
- show policer
clear firewall

List of Syntax

Syntax on page 2536
Syntax (EX Series Switches) on page 2536

Syntax

clear firewall (all | counter counter-name | filter filter-name | log (all | logical-system-name ) | logical-system logical-system-name)

Syntax (EX Series Switches)
clear firewall (all | counter counter-name | filter filter-name | log (all | logical-system-name) | policer counter (all | counter-id counter-index))

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
logical-system option introduced in Junos OS Release 9.3.
log option introduced before Junos OS Release 11.4.

Description

Clear statistics about configured firewall filters.

When you clear the counters of a filter, this impacts not only the counters shown by the CLI, but also the ones tracked by SNMP2.

Subscriber management uses firewall filters to capture and report the volume-based service accounting counters that are used for subscriber billing. The clear firewall command also clears the service accounting counters that are reported to the RADIUS accounting server. For this reason, you must be cautious in specifying which firewall statistics you want to clear.

NOTE: The clear firewall command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for graceful Routing Engine switchover (GRES).

If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the prefix-action action on matched packets, wait at least 5 seconds before you enter the show firewall prefix-action-stats command. A 5-second pause between issuing the clear firewall and show firewall prefix-action-stats commands avoids a possible timeout of the show firewall prefix-action-stats command.

Options

all—Clear the packet and byte counts for all filters. On EX Series switches, this option also clears the packet counts for all policer counters.

counter counter-name—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.

filter filter-name—Clear the packet and byte counts for the specified firewall filter.
log (all | logical-system-name) — Clear log entries for IPv4 firewall filters that have then log as an action. Use log all to clear all log entries or log logical-system-name to clear log entries for the specified logical system.

logical-system logical-system-name — Clear the packet and byte counts for the specified logical system.

policer counter (all | counter-id counter-index) — (EX8200 switches only) Clear all policer counters using the policer counter all command, or clear a specific policer counter using the policer counter counter-id counter-index command. The value of counter-index can be 0, 1, or 2.

Required Privilege Level

Related Documentation

- show firewall on page 2538

List of Sample Output

clear firewall all on page 2537
clear firewall (counter counter-name) on page 2537
clear firewall (filter filter-name) on page 2537
clear firewall (policer counter all) (EX8200 Switch) on page 2537
clear firewall (policer counter counter-id counter-index) (EX8200 Switch) on page 2537

Sample Output

clear firewall all

    user@host> clear firewall all

clear firewall (counter counter-name)

    user@host> clear firewall counter port-filter-counter

clear firewall (filter filter-name)

    user@host> clear firewall filter ingress-port-filter

clear firewall (policer counter all) (EX8200 Switch)

    user@switch> clear firewall policer counter all

clear firewall (policer counter counter-id counter-index) (EX8200 Switch)

    user@switch> clear firewall policer counter counter-id 0
show firewall

List of Syntax  Syntax on page 2538
Syntax (EX Series Switches) on page 2538

Syntax  show firewall
  <application (CFM | eswd | RMPS)>
  <counter counter-name>
  <detail>
  <filter filter-name>
  <filter regex regular-expression>
  <logical-system (all | logical-system-name)>
  <terse>

Syntax (EX Series Switches)  show firewall
  <application (CFM | eswd | RMPS)>
  <counter counter-name>
  <detail>
  <filter filter-name>
  <filter regex regular-expression>
  <log < (detail | interface interface-name)>
  <policer counters < (detail | counter-id counter-index <detail>)>
  <terse>

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option logical-system introduced in Junos OS Release 9.3.
Option terse introduced in Junos OS Release 9.4.
Option policer counters introduced in Junos OS Release 12.2 for EX Series switches.
Option detail introduced in Junos OS Release 12.3 for EX Series switches.
Option detail introduced in Junos OS Release 14.1 for MX Series routers.
Option regex regular-expression introduced in Junos OS Release 14.2.
Option lsp introduced in Junos OS Evolved Release 18.3R1.

Description  Display enhanced statistics and counters for all configured firewall filters.

If you query for options on the `show firewall filter` command, on Junos OS systems, you will see this output, which includes the configured Flowspec filters:

```
show firewall filter ?
```

Possible completions:

<table>
<thead>
<tr>
<th>Completion</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filtername&gt;</td>
<td>Filter name</td>
</tr>
<tr>
<td><strong>flowspec_default_inet</strong></td>
<td># Flowspec filter name</td>
</tr>
<tr>
<td>application</td>
<td>Owner application</td>
</tr>
<tr>
<td>counter</td>
<td>Counter name</td>
</tr>
<tr>
<td>logical-system</td>
<td>Name of logical system, or 'all'</td>
</tr>
<tr>
<td>regex</td>
<td>Show filter using regular expression</td>
</tr>
<tr>
<td>version</td>
<td>Show filter version installed</td>
</tr>
</tbody>
</table>
However, on Junos OS Evolved systems, the Flowspec filters names are not shown here. To view Flowspec filters, use the `show firewall application routing` command.

**Options**

- `none`—(Optional) Display statistics and counters for all configured firewall filters and counters. For EX Series switches, this command also displays statistics about all configured policers.
- `application (CFM | eswd | RMPS)`—(Optional) Show firewall elements owned by the selected software component:
  - Connectivity Fault Management (CFM)
  - Ethernet switching daemon (eswd)—Shows only on devices that support it.
  - Resource Management and Packet Steering (RMPS)
- `counter counter-name`—(Optional) Name of a filter counter.
- `detail`—(EX Series switches and MX Series routers only) (Optional) Display firewall filter statistics and enhanced policer statistics and counters.
- `filter filter-name`—(Optional) Name of a configured filter.
- `filter regex regular-expression`—(Optional) Regular expression that matches the names of a subset of filters.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `log`—(Optional) Display log entries for firewall filters.
- `log < (detail | interface interface-name) >`—(EX Series switches only) (Optional) Display detailed log entries of firewall activity or log information about a specific interface.
- `policer counters < (detail | counter-id counter-index <detail>) >`—(EX8200 switches only) (Optional) Display enhanced policer counter statistics in brief or in detail.
- `terse`—(Optional) Display firewall filter names only.

**Required Privilege**

- view

**Related Documentation**

- clear firewall on page 2536
- show firewall log on page 2547
- Verifying That Firewall Filters Are Operational
- Verifying That Policers Are Operational
- show policer on page 2554
- Enhanced Policer Statistics Overview
- enhanced-policer

### List of Sample Output
- show firewall filter (MX Series Router and EX Series Switch) on page 2542
- show firewall filter (non MX Series Router and EX Series Switch) on page 2542
- show firewall filter (Dynamic Input Filter) on page 2542
- show firewall (Logical Systems) on page 2542
- show firewall (counter counter-name) on page 2543
- show firewall log on page 2543
- show firewall policer counters (EX8200 Switch) on page 2543
- show firewall policer counters (detail) (EX8200 Switch) on page 2544
- show firewall policer counters (counter-id counter-index) (EX8200 Switch) on page 2544
- show firewall policer counters (counter-id counter-index detail) (EX8200 Switch) on page 2544
- show firewall detail on page 2545
- show firewall application cfm (Junos OS Evolved) on page 2545

### Output Fields
Table 198 on page 2540 lists the output fields for the `show firewall` command. Output fields are listed in the approximate order in which they appear.

**Table 198: show firewall Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Name of a filter that has been configured with the <code>filter</code> statement at the <code>[edit firewall]</code> hierarchy level.</td>
</tr>
<tr>
<td></td>
<td>Except on EX Series switches:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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 (<code>_</code>) characters and the name of the logical system (for example, <code>_ls1/filter1</code>).</td>
</tr>
<tr>
<td></td>
<td>- When a service filter is displayed that uses a service set, the separator between the service-set name and the service-filter name is a semicolon (<code>;</code>).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For bridge family filter, the <code>ip-protocol</code> match criteria is supported only for IPv4 and not for IPv6. This is applicable for line cards that support the Junos Trio chipset, such as the MX 3D MPC line cards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Counters</th>
<th>Display filter counter information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Name—Name of a filter counter that has been configured with the <code>counter</code> firewall filter action.</td>
</tr>
<tr>
<td></td>
<td>- Bytes—Number of bytes that match the filter term under which the <code>counter</code> action is specified.</td>
</tr>
<tr>
<td></td>
<td>- Packets—Number of packets that matched the filter term under which the <code>counter</code> action is specified.</td>
</tr>
</tbody>
</table>

**NOTE:** On M and T Series routers, firewall filters cannot count `ip-options` packets on a per option type and per interface basis. A limited workaround is to use the `show pfe statistics ip options` command to see `ip-options` statistics on a per Packet Forwarding Engine (PFE) basis. See `show pfe statistics ip` for sample output.
Table 198: show firewall Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policers</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>—(For two-color policers on MX Series routers and EX Series switches, and for hierarchical policers on interfaces hosted on MICs and MPCs in MX Series routers) 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. For other combinations of policer type, device, and line card type, this field is blank.</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>
<tr>
<td>Policer Counter Index</td>
<td>(EXB200 switch only) Global management counter ID. The counter ID value (counter-index) can be 0, 1, or 2.</td>
</tr>
<tr>
<td>Green</td>
<td>(EXB200 switch only) Number of packets within the limits. The number of packets is smaller than the committed information rate (CIR).</td>
</tr>
<tr>
<td>Yellow</td>
<td>(EXB200 switch only) Number of packets partially within the limits. The number of packets is greater than the CIR, but the burst size is within the excess burst size (EBS) limit.</td>
</tr>
<tr>
<td>Discard</td>
<td>(EXB200 switch only) Number of discarded packets.</td>
</tr>
<tr>
<td>Bytes</td>
<td>(EXB200 switch only) Number of green, yellow, red, or discarded packets in bytes.</td>
</tr>
<tr>
<td>Packets</td>
<td>(EXB200 switch only) Number of green, yellow, red, or discarded packets.</td>
</tr>
<tr>
<td>Filter name</td>
<td>(EXB200 switch only) Name of the filter with a term associated to a policer.</td>
</tr>
<tr>
<td>Term name</td>
<td>(EXB200 switch only) Name of the term associated with a policer.</td>
</tr>
<tr>
<td>Policer name</td>
<td>(EXB200 switch only) Name of the policer that is associated with a global management counter.</td>
</tr>
<tr>
<td>P1-t1</td>
<td>• OOS packet statistics for packets that are marked out-of-specification (out-of-spec) by the policer. Changes to all packets that have out-of-spec actions, such as discard, color marking, or forwarding-class, are included in this counter.</td>
</tr>
<tr>
<td></td>
<td>• Offered packet statistics for traffic subjected to policing.</td>
</tr>
<tr>
<td></td>
<td>• Transmitted packet statistics for traffic that is not discarded by the policer. When the policer action is discard, the statistics are the same as the in-spec statistics; when the policer action is non-discard (loss-priority or forwarding-class), the statistics are included in this counter.</td>
</tr>
</tbody>
</table>
Sample Output

show firewall filter (MX Series Router and EX Series Switch)

user@host> show firewall filter test

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Counter-2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Policers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policer-1</td>
<td>2770</td>
<td>70</td>
</tr>
</tbody>
</table>

show firewall filter (non MX Series Router and EX Series Switch)

user@host> show firewall filter test

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Counter-2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Policers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policer-1</td>
<td></td>
<td>70</td>
</tr>
</tbody>
</table>

show firewall filter (Dynamic Input Filter)

user@host> show firewall filter dfwd-ge-5/0/0.1-in

Filter: dfwd-ge-5/0/0.1-in

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1-ge-5/0/0.1-in</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show firewall (Logical Systems)

user@host> show firewall

Filter: __lr1/test

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp</td>
<td>420</td>
<td>5</td>
</tr>
</tbody>
</table>

Filter: __default_bpdu_filter__

Filter: __lr1/inet_filter1

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet_tcp_count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inet_udp_count</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

Filter: __lr1/inet_filter2

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>inet_icmp_count</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>inet_pim_count</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter: __lr2/inet_filter1
show firewall (counter counter-name)

user@host> show firewall counter icmp-counter

Filter: ingress-port-voip-class-filter

Counters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-counter</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show firewall log

user@host> show firewall log

Log:

<table>
<thead>
<tr>
<th>Time</th>
<th>Filter</th>
<th>Action</th>
<th>Interface</th>
<th>Protocol</th>
<th>Src Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00:53</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:52</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:51</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:50</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:49</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:48</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
<tr>
<td>08:00:47</td>
<td>pfe</td>
<td>R</td>
<td>ge-1/0/1.0</td>
<td>ICMP</td>
<td>192.168.3.5</td>
</tr>
</tbody>
</table>

show firewall policer counters (EX8200 Switch)

user@switch> show firewall policer counters

Policer Counter Index 0:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green:</td>
<td>73</td>
<td>15914</td>
</tr>
<tr>
<td>Yellow:</td>
<td>9</td>
<td>1962</td>
</tr>
<tr>
<td>Discard:</td>
<td>119</td>
<td>25942</td>
</tr>
</tbody>
</table>

Policer Counter Index 1:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yellow:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discard:</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Policer Counter Index 2:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green:</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**show firewall policer counters (detail) (EX8200 Switch)**

```
user@switch> show firewall policer counters detail

Policer Counter Index 0:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter name</th>
<th>Term name</th>
<th>Policer name</th>
</tr>
</thead>
<tbody>
<tr>
<td>myfilter</td>
<td>polcr-term-1</td>
<td>myfilter-polcr-1</td>
</tr>
<tr>
<td>inet-filter-ae</td>
<td>ae-snmp</td>
<td>policer-1</td>
</tr>
<tr>
<td>inet-filter-ae</td>
<td>ae-ssh</td>
<td>policer-2</td>
</tr>
</tbody>
</table>

Policer Counter Index 1:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
</tr>
</tbody>
</table>

Policer Counter Index 2:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
</tr>
</tbody>
</table>

**show firewall policer counters (counter-id counter-index) (EX8200 Switch)**

```
user@switch> show firewall policer counters counter-id 0

Policer Counter Index 0:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
</tr>
</tbody>
</table>

**show firewall policer counters (counter-id counter-index detail) (EX8200 Switch)**

```
user@switch> show firewall policer counters counter-id 0 detail

Policer Counter Index 0:

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter name</th>
<th>Term name</th>
<th>Policer name</th>
</tr>
</thead>
<tbody>
<tr>
<td>myfilter</td>
<td>polcr-term-1</td>
<td>myfilter-polcr-1</td>
</tr>
<tr>
<td>inet-filter-ae</td>
<td>ae-snmp</td>
<td>policer-1</td>
</tr>
<tr>
<td>inet-filter-ae</td>
<td>ae-ssh</td>
<td>policer-2</td>
</tr>
</tbody>
</table>
show firewall detail

```bash
user@host> show firewall detail
Filter: __default_bpdu_filter__

Filter: foo
Counters:
Name                    Bytes     Packets
  c1                 17652140   160474

Policers:
Name                    Bytes     Packets
  P1-t1                   0         18286
  OOS                   0           18446744073709376546
  Offered                0       18446744073709358260
```

show firewall application cfm (Junos OS Evolved)

```bash
user@host> show firewall application cfm
Filter: __cfm_filter_et-0/0/0__
Counters:
Name                    Bytes     Packets
  __cfm_cc_term_lvl_0__      0          0
  __cfm_cc_term_lvl_1__      0          0
  __cfm_cc_term_lvl_2__      0          0
  __cfm_cc_term_lvl_3__      0          0
  __cfm_cc_term_lvl_4__      0          0
  __cfm_cc_term_lvl_5__      0          0
  __cfm_cc_term_lvl_6__      0          0
  __cfm_cc_term_lvl_7__      0          0
  __cfm_ethtype_term__       0          0
  __cfm_lt_term_lvl_0__      0          0
  __cfm_lt_term_lvl_1__      0          0
  __cfm_lt_term_lvl_2__      0          0
  __cfm_lt_term_lvl_3__      0          0
  __cfm廖_term_lvl_4__      0          0
  __cfm廖_term_lvl_5__      0          0
  __cfm廖_term_lvl_6__      0          0
  __cfm廖_term_lvl_7__      0          0
  __cfm_uceast_term_536__    0          0
```
show firewall filter version

**Syntax**
```
show firewall filter version <filter-name>
```

**Release Information**
Command introduced in Junos OS Release 10.2R2.

**Description**
Display the version number of the installed firewall filter in the Routing Engine.

**Options**
- `none`—(Optional) Display the version number of all installed firewall filters.
- `filter-name`—(Optional) Name of a configured filter. If you specify the name of a filter, only the version number of that filter is displayed.

**Additional Information**
The initial version number is 1. This number increments by one when you modify the firewall filter settings or an associated prefix action. The maximum version number is 4,294,967,295. When the version number reaches 4,294,967,295, this number is reset to 1.

**Required Privilege**
`view`

**List of Sample Output**
`show firewall filter version on page 2546`

**Output Fields**
Table 199 on page 2546 lists the output fields for the `show firewall filter version` 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>Filter</td>
<td>Name of a filter that has been configured with the <code>filter</code> statement at the <code>[edit firewall]</code> hierarchy level.</td>
</tr>
<tr>
<td>Version</td>
<td>Display the version number of the firewall filter.</td>
</tr>
</tbody>
</table>

**Sample Output**
`show firewall filter version`
```
user@host> show firewall filter version
Filter version information :
Filter  Version
test   10
```

Copyright © 2019, Juniper Networks, Inc.
show firewall log

List of Syntax
Syntax on page 2547
Syntax (EX Series Switches) on page 2547

Syntax
show firewall log
<detail>
<extensive>
<interface interface-name>
<logical-system (logical-system-name | all)>

Syntax (EX Series Switches)
show firewall log
<interface interface-name>

Release Information
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
extensive option introduced in Junos OS Release 16.1.  
logical-system option introduced in Junos OS Release 9.3.

Description
Display log information about firewall filters.

Options
none—Display log information about firewall filters.
detail—(Optional) Display detailed information.
extensive—(Optional) Display hex dump of packet captured by log action.
interface interface-name—(Optional) Display log information about a specific interface.
logical-system (logical-system-name | all)—(Optional) Perform this operation on all logical systems or on a particular system.

Required Privilege
view

List of Sample Output
show firewall log on page 2548
show firewall log detail on page 2548
show firewall log extensive on page 2549

Output Fields
Table 200 on page 2547 lists the output fields for the show firewall log command. Output fields are listed in the approximate order in which they appear.

Table 200: show firewall log Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Log</td>
<td>Time that the event occurred.</td>
</tr>
</tbody>
</table>
### Table 200: show firewall log Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Filter              | • Displays the name of a configured firewall filter or service filter only if the packet hit the filter's log action in a kernel filter (in the control plane). For any traffic that reaches the Routing Engine, the packets hit the log action in the kernel.  
• For all other logged packets (packet hit the filter's log action in the Packet Forwarding Engine), this field displays pfe instead of a configured filter name. |
| Filter Action       | Filter action:                                                                                                                                                                                                      |
|                     | • A—Accept                                                                                                                                                                                                          |
|                     | • D—Discard                                                                                                                                                                                                         |
|                     | • R—Reject                                                                                                                                                                                                         |
| Name of interface   | • Displays a physical interface name if the packet arrived at a port on a line card.                                                                                                                                  |
|                     | • Displays local if the packet was generated by the device's internal Ethernet interface, em1 or fxp1, which connects the Routing Engine with the router's packet-forwarding components.                                       |
| Name of protocol    | Packet's protocol name: egp, gre, icmp, ipip, ospf, pim, rsvp, tcp, or udp.                                                                                                                                          |
| Packet length       | Length of the packet.                                                                                                                                                                                                |
| Source address      | Packet's source address.                                                                                                                                                                                              |
| Destination address | Packet's destination address and port.                                                                                                                                                                               |

### Sample Output

**show firewall log**

```
user@host>show firewall log
Time      Filter    Action Interface     Protocol  Src Addr      Dest Addr
13:10:12  pfe       D      r1sq0.902     ICMP      192.0.2.2   192.0.2.1
13:10:11  pfe       D      r1sq0.902     ICMP      192.0.2.2   192.0.2.1
```

**show firewall log detail**

```
user@host> show firewall log detail
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
```
Name of protocol: TCP, Packet Length: 1020, Source address: 203.0.113.108:829, Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 203.0.113.108:829, Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 203.0.113.108:829, Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 203.0.113.108:829, Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 203.0.113.108:829, Destination address: 192.168.70.66:513
....

show firewall log extensive

user@host> show firewall log extensive

Time of Log: 2016-01-17 22:16:21 PST, Filter: pfe, Filter action: accept, Name of interface: xe-0/0/1.0
Name of protocol: UDP, Packet Length: 98, Source address: 203.0.113.1, Destination address: 203.0.113.1
  00-0F: 00 01 03 ee ee ff 00 01 - 09 22 55 ee 81 00 02 58
  10-1F: 08 00 45 00 00 62 00 00 - 00 00 40 11 77 8a 01 00
  20-2F: 00 01 02 00 00 01 1c 00 - 1c 00 00 4e 19 83 00 01
  30-3F: 02 03 04 05 06 07 08 09 - 0a 0b 0c 0d 0e 0f 10 11
  40-4F: 12 13 14 15 16 17 18 19 - 1a 1b 1c 1d 1e 1f 20 21
  50-5F: 22 23 24 25 26 27 28 29 - 2a 2b 00 00 00 00 00 00
  60-6F: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
  70-7F: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00
show firewall prefix-action-stats

List of Syntax
Syntax (filter-specific mode) on page 2550
Syntax (term-specific mode) on page 2550

Syntax (filter-specific mode)
show firewall prefix-action-stats filter filter-name prefix-action prefix-action-name
<from number to number>
<logical-system (logical-system-name | all)>

Syntax (term-specific mode)
show firewall prefix-action-stats filter filter-name prefix-action prefix-action-name-term-name
<from number to number>
<logical-system (logical-system-name | all)>

Release Information
Command introduced before Junos OS Release 7.4.
logical-system option introduced in Junos OS Release 9.3.

Description
Display prefix action statistics about configured firewall filters.

If you clear statistics for firewall filters that are applied to MPCs and that also use the prefix-action action on matched packets, wait at least 5 seconds before you enter the show firewall prefix-action-stats command. A 5-second pause between issuing the clear firewall and show firewall prefix-action-stats commands avoids a possible timeout of the show firewall prefix-action-stats command.

By default, policers operate in term-specific mode.

See Filter-Specific Policer Overview for information about how to configure policers in filter-specific mode.

Options
filter filter-name—Name of a filter.
prefix-action prefix-action-name—Name of a prefix action.
from number to number—(Optional) Starting and ending counter or policer.
logical-system (logical-system-name | all)—(Optional) Perform this operation on all logical systems or on a particular system.

Required Privilege
view

Related Documentation
• clear firewall on page 2536

List of Sample Output
show firewall prefix-action-stats on page 2551
Output Fields  Table 201 on page 2551 lists the output fields for the show firewall prefix-action-stats command. Output fields are listed in the approximate order in which they appear.

Table 201: show firewall prefix-action-stats Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Filter name.</td>
</tr>
</tbody>
</table>

Filters configured for logical systems include the name of the filter prefixed with the two underscore characters (__) and the name of the logical system (for example, __ls1/filter1).

Sample Output

The following sample output assumes that the policer act1 is in term mode and that there is a term named term1 configured in the firewall filter test.

```bash
user@host> show firewall prefix-action-stats filter test prefix-action act1-term1 from 0 to 9
Filter: test
Counters:
Name       | Bytes | Packets |
---------- |------- |---------|
act1-0     | 0      | 0        |
act1-1     | 0      | 0        |
act1-2     | 0      | 0        |
act1-3     | 0      | 0        |
act1-4     | 0      | 0        |
act1-5     | 0      | 0        |
act1-6     | 0      | 0        |
act1-7     | 0      | 0        |
act1-8     | 0      | 0        |
act1-9     | 0      | 0        |
Policers:
Name       | Bytes | Packets |
---------- |------- |---------|
act1-0     | 0      | 0        |
act1-1     | 0      | 0        |
act1-2     | 0      | 0        |
act1-3     | 0      | 0        |
act1-4     | 0      | 0        |
act1-5     | 0      | 0        |
act1-6     | 0      | 0        |
act1-7     | 0      | 0        |
act1-8     | 0      | 0        |
act1-9     | 0      | 0        |
```
show firewall templates-in-use

Syntax

show firewall templates-in-use

Release Information
Command introduced in Junos OS Release 12.3.

Description
Display the names of configured filter templates that are currently in use by dynamic subscribers and the number of times each template is referenced.

Required Privilege
view

Related Documentation
• clear firewall on page 2536
• show firewall log on page 2547

List of Sample Output
show firewall templates-in-use on page 2553

Output Fields
Table 202 on page 2552 lists the output fields for the show firewall templates-in-use command. Output fields are listed in the approximate order in which they appear.

Table 202: show firewall templates-in-use Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Template</td>
<td>Name of a filter that has been configured using the filter statement at either the [edit firewall] or [edit dynamic-profiles profile-name firewall] hierarchy and is being used as a template for dynamic subscriber filtering.</td>
</tr>
<tr>
<td>Reference Count</td>
<td>Number of times the filter has been referenced by subscribers accessing the network.</td>
</tr>
</tbody>
</table>
## Sample Output

### show firewall templates-in-use

```
user@host> show firewall templates-in-use

<table>
<thead>
<tr>
<th>Filter Template</th>
<th>Reference Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>egressFilter</td>
<td>10</td>
</tr>
<tr>
<td>ingressFilter</td>
<td>10</td>
</tr>
<tr>
<td>dfilter</td>
<td>5</td>
</tr>
<tr>
<td>dfilter-pol</td>
<td>5</td>
</tr>
</tbody>
</table>
```
show policer

Syntax

show policer
<detail>
<policer-name>

Release Information

Command introduced before Junos OS Release 7.4.
The command show policer detail was introduced in Junos OS Release 12.3.

Description

Display the number of policed packets for a given policer or an aggregate policer. An aggregate policer is an aggregate of different policers on the same logical interface.

Options
detail—(Optional) Display additional statistics and counters. Requires the enhanced-policer statement to be enabled at the [edit chassis] hierarchy level.

NOTE: show policer detail is not available for the following counters:
three color policers, hierarchical policers, prefix-specific actions, LSP policers and other nexthop policers, and fast-update-filters on devices running MPC1 or MPC2 line cards.

policer-name—(Optional) Display the number of policed packets for the specified policer.
<null>—Displays the number of policed packets for all configured policers.

Required Privilege Level

view

List of Sample Output

show policer (MX Series) on page 2555
show policer (non-MX Series Router) on page 2555
show policer (Aggregate Policer, non MX Series Router) on page 2556
show policer detail (MX Series Router running MPC 1 or MPC 2 line cards) on page 2556

Output Fields

Table 203 on page 2555 lists the output fields for the show policer command. Output fields are listed in the approximate order in which they appear.
Table 203: show policer Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the policer. Policier detail also includes the following statistics:</td>
</tr>
<tr>
<td></td>
<td>OOS—Packet statistics for packets that are marked out-of-specification by the policer. Changes to all packets that have out-of-specification actions, such as discard, color marking, or forwarding-class, are included in this counter.</td>
</tr>
<tr>
<td></td>
<td>Offered—Packet statistics for traffic subjected to policing.</td>
</tr>
<tr>
<td></td>
<td>Transmitted—Packet statistics for traffic that is not discarded by the policer. When the policer action is discard, the statistics are the same as the within-specification statistics; when the policer action is non-discard (loss-priority or forwarding-class), the statistics are included in this counter.</td>
</tr>
<tr>
<td>Bytes</td>
<td>• (For two-color policers on MX Series routers, and for hierarchical policers on MS-DPC, MIC, and MPC interfaces on MX Series routers)—Total number of bytes policed by the specified policer. For other combinations of policer type, device, and line card type, this field is blank.</td>
</tr>
<tr>
<td></td>
<td>• (T Series and M10i)—Not applicable. The Bytes information is not displayed.</td>
</tr>
<tr>
<td>Packets</td>
<td>Total number of packets policed by the specified policer.</td>
</tr>
</tbody>
</table>

Sample Output

**show policer (MX Series)**

```
user@host> show policer
Policers:
Name                                                Bytes              Packets
__default_arp_policer__                            314520                 5242
pol-2M-ge-1/2/0.1-inet-i                           10372300               103723
pol-2M-ge-1/2/0.1-inet6-i                          7727800                77278
pol-2M-ge-1/2/0.1-mpls-i                           7070336                67984
pol-2M-ge-1/2/0.1001-vpls-i                        65153700               651537
pol-2M-ge-1/2/0.2001-vpls-i                        65180900               651809
pol-2M-ge-1/2/0.3001-ccc-i                         62202144               647939
```

**show policer (non MX Series Router)**

```
user@host> show policer
Policers:
Name                                                Bytes              Packets
__default_arp_policer__                                NA                 5242
pol-2M-ge-1/2/0.1-inet-i                               NA               103723
pol-2M-ge-1/2/0.1-inet6-i                              NA                77278
pol-2M-ge-1/2/0.1-mpls-i                               NA                67984
pol-2M-ge-1/2/0.1001-vpls-i                           65180900               651809
pol-2M-ge-1/2/0.2001-vpls-i                           65153700               651537
pol-2M-ge-1/2/0.3001-ccc-i                            62202144               647939
```

Chapter 28: Firewall Filter Operational Commands

Copyright © 2019, Juniper Networks, Inc.
### show policer (Aggregate Policer, non MX Series Router)

```plaintext
user@host> show policer

<table>
<thead>
<tr>
<th>Policers:</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default_arp_policer</strong></td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td>P1-ae0.0-log_int-o</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td>P2-ge-7/0/2.0-inet-o</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td>P2-ge-7/0/2.0-inet6-o</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-term</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc1</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc1</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc1</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc2</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc1</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc2</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td><strong>policer_tmpl</strong>-fc3</td>
<td>NA</td>
<td>0</td>
</tr>
</tbody>
</table>
```

### show policerdetail (MX Series Router running MPC 1 or MPC 2 line cards)

```plaintext
user@host> show policerdetail

<table>
<thead>
<tr>
<th>Policers:</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default_arp_policer</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Offered</td>
<td>0</td>
<td>496</td>
</tr>
<tr>
<td>Transmitted</td>
<td>0</td>
<td>496</td>
</tr>
<tr>
<td>P1-ae0.0-log_int-o</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOS</td>
<td>0</td>
<td>111329</td>
</tr>
<tr>
<td>Offered</td>
<td>0</td>
<td>111188</td>
</tr>
<tr>
<td>Transmitted</td>
<td>0</td>
<td>99859</td>
</tr>
</tbody>
</table>
```
Layer 2 Bridging and Switching Operational Commands

- clear bridge mac-table
- clear error bpdu interface
- clear error mac-rewrite
- show bridge domain
- show bridge flood
- show bridge mac-table
- show bridge statistics
- show l2-learning global-information
- show l2-learning global-mac-count
- show l2-learning instance
- show l2-learning interface
- show mac-rewrite interface
### clear bridge mac-table

**Syntax**

```
clear bridge mac-table
  <bridge-domain (all | bridge-domain-name)>
  <instance instance-name>
  <interface interface-name>
  <learning-vlan id (all-vlan | learning-vlan-id)>
  <mac-address>
```

**Release Information**

Command introduced in Junos OS Release 8.4.

**Description**

(MX Series routers only) Clear learned Layer 2 address information from the media access control (MAC) address table.

**Options**

- **none**—Clear all learned Layer 2 address information from the MAC address table.
- **bridge-domain (all | bridge-domain-name)**—(Optional) Clear learned Layer 2 MAC addresses for all bridging domains or for the specified bridging domain.
- **instance instance-name**—(Optional) Clear learned Layer 2 MAC addresses for the specified routing instance.
- **interface interface-name**—(Optional) Clear learned Layer 2 MAC addresses for the specified interface.
- **learning-vlan-id (all-vlan | learning-vlan-id)**—(Optional) Clears learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.
- **mac-address**—(Optional) Clear the specified learned Layer 2 address from the MAC address table.

**Required Privilege Level**

clear

**List of Sample Output**

| clear bridge mac-table on page 2558 |

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear bridge mac-table

user@host> clear bridge mac-table
```


### clear error bpdu interface

**List of Syntax**  
- MX Series on page 2559  
- QFX Series, EX Series, NFX Series on page 2559

**MX Series**  
`clear error bpdu interface interface-name`

**QFX Series, EX Series, NFX Series**  
`clear error bpdu interface (all | interface-name)`

**Release Information**  
- Command introduced in Junos OS Release 9.4.  
- Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
- Command supports `all` option in Junos OS Release 15.1 for EX Series switches.

**Description**  
Clear a bridge protocol data unit (BPDU) error condition caused by the detection of a possible bridging loop from Spanning Tree Protocol (STP) operation.

**Required Privilege**  
`clear`

**Related Documentation**  
- `Configuring BPDU Protection on ACX Router, EX Switch and MX Router Edge Ports`
- `Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure)`

**List of Sample Output**  
`clear error bpdu interface ge-1/1/1 on page 2559`

**Output Fields**  
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear error bpdu interface ge-1/1/1
user@host> clear error bpdu interface ge-1/1/1
```
clear error mac-rewrite

Syntax  
clear error mac-rewrite
<interface interface-name>

Release Information  
Command introduced in Junos OS Release 9.1.
Command introduced in Junos OS Release 14.1X53-D10 and 17.3R1 for EX4300 switches.
Command introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Command introduced in Junos OS Release 17.4R1 for EX4600 switches.
Command introduced in Junos OS Release 19.1R1 for QFX5200 switches.

Description  
Clear a MAC rewrite error condition caused by the reception of tunneled protocol packets on an interface with Layer 2 protocol tunneling enabled.

On interfaces with L2PT configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless there is a network topology or configuration error. Any such interface receiving an L2PT packet becomes “Disabled”, and must subsequently be re-enabled by clearing the error with this command.

Options  
interface interface-name — (Optional) Clear the MAC rewrite error condition for the specified interface.

Required Privilege Level  
clear

Related Documentation  
- Configuring Layer 2 Protocol Tunneling
- Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling
- show mac-rewrite interface on page 2586

List of Sample Output  
clear error mac-rewrite interface on page 2560

Output Fields  
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error mac-rewrite interface

user@host> clear error mac-rewrite interface ge-1/0/1
**show bridge domain**

**Syntax**

```
show bridge domain
<brief | detail | extensive>
<bridge-domain (all | domain-name)>
<instance instance-name>
<operational>
```

**Release Information**

Command introduced in Junos OS Release 8.4.

**Description**

(MX Series routers only) Display bridge domain information.

**Options**

- none—Display information for all bridge domains.
- brief | detail | extensive—(Optional) Display the specified level of output.
- bridge-domain (all | domain-name)—(Optional) Display information about all bridge domains or the specified bridge domain.
- instance instance-name—(Optional) Display information for the specified routing instance.
- operational—(Optional) Display information for the operational routing instances.

**Required Privilege**

- view

**List of Sample Output**

- show bridge domain on page 2561
- show bridge domain brief on page 2561
- show bridge domain detail on page 2562

**Sample Output**

**show bridge domain**

```
show bridge domain

<table>
<thead>
<tr>
<th>Instance</th>
<th>Bridging Domain</th>
<th>Type</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>Primary Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan100</td>
<td>bridge</td>
<td>2</td>
</tr>
<tr>
<td>vs1</td>
<td>Primary Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan200</td>
<td>bridge</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**show bridge domain brief**

```
show bridge domain brief

<table>
<thead>
<tr>
<th>Instance</th>
<th>Bridging Domain</th>
<th>Type</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs1</td>
<td>Primary Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>bridge.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan100</td>
<td>bridge</td>
<td>2</td>
</tr>
</tbody>
</table>
```

Copyright © 2019, Juniper Networks, Inc.
### show bridge domain detail

```
user@host> show bridge domain detail

Routing Instance: vs1
  Bridging Domain: vlan100
  Router ID: 0.0.0.0
  Type: bridge  State: Active
  Interfaces:
    ge-11/0/3.0
    ge-11/1/4.100
    ge-11/1/1.100
    ge-11/1/0.100
    xe-10/2/0.100
    xe-10/0/0.100
  Tables:
    bridge.0 : 2 macs (2 active)

Routing Instance: vs1
  Bridging Domain: vlan200
  Router ID: 0.0.0.0
  Type: bridge  State: Active
  Interfaces:
    ge-11/1/0.200
    ge-11/1/1.200
    ge-11/1/4.200
    xe-10/0/0.200
    xe-10/2/0.200
  Tables:
    bridge.0 : 0 macs (0 active)
```
show bridge flood

Syntax

show bridge flood
  <brief | detail | extensive>
  <bridge-domain domain-name>
  <event-queue>
  <instance instance-name>
  <route (all-ce-flood | all ve-flood | alt-root-flood | bd-flood | mlp-flood | re-flood)>

Release Information

Command introduced in Junos OS Release 8.4.

Description

(MX Series routers only) Display bridging flooding information.

Options

none—Display all bridging flooding information for all bridging domains.

brief | detail | extensive—(Optional) Display the specified level of output.

bridge-domain domain-name—(Optional) Display bridging flooding information for the specified bridge domain.

event-queue—(Optional) Display the queue of pending bridge flood events.

instance instance-name—(Optional) Display bridging flooding information for the specified routing instance.

route (all-ce-flood | all ve-flood | alt-root-flood | bd-flood | mlp-flood | re-flood)—(Optional) Display the following:

  • all-ce-flood—Display the route for flooding traffic to all customer edge routers if no-local-switching is enabled.
  • all-ve-flood—Display the route for flooding traffic to all VPLS edge routers if no-local-switching is enabled.
  • alt-root-flood—Display the Spanning Tree Protocol (STP) alt-root flooding route used for the interface.
  • bd-flood—Display the route for flooding traffic of a bridge domain if no-local-switching is not enabled.
  • mlp-flood—Display the route for flooding traffic to MAC learning chips.
  • re-flood—Display the route for Routing Engine flooding to all interfaces.

Required Privilege Level

view

List of Sample Output

show bridge flood on page 2564
show bridge flood brief on page 2564
show bridge flood detail on page 2564
Show bridge flood extensive on page 2565

Output Fields to be provided

Sample Output

```
show bridge flood

Name: __juniper_private1__
CEs: 0
VEs: 0
Flood Routes:
Prefix    Type          Owner                 NhType          NhIndex
0x36/16   MLP_FLOOD     __vs1+vlan100__       flood           426
0x3a/16   MLP_FLOOD     __vs1+vlan200__       flood           428
Name: vs1::vlan100
CEs: 6
VEs: 0
Flood Routes:
Prefix    Type          Owner                 NhType          NhIndex
0x35/16   ALL_FLOOD     __vs1+vlan100__       flood           425
0x35/16   RE_FLOOD      __vs1+vlan100__       flood           425
0x3780/17 ALT_ROOT_RT   ge-11/0/3.0            flood           425
0x3b80/17 ALT_ROOT_RT   ge-11/1/1.100         flood           425
0x3c80/17 ALT_ROOT_RT   ge-11/1/1.100         flood           425
0x3d80/17 ALT_ROOT_RT   ge-11/1/0.100         flood           425
0x3e80/17 ALT_ROOT_RT   xe-10/2/0.100         flood           425
0x3f80/17 ALT_ROOT_RT   xe-10/0/0.100         flood           425
Name: vs1::vlan200
CEs: 5
VEs: 0
Flood Routes:
Prefix    Type          Owner                 NhType          NhIndex
0x39/16   ALL_FLOOD     __vs1+vlan200__       flood           427
0x39/16   RE_FLOOD      __vs1+vlan200__       flood           427
0x4180/17 ALT_ROOT_RT   ge-11/1/0.200         flood           427
0x4080/17 ALT_ROOT_RT   ge-11/1/1.200         flood           427
0x4280/17 ALT_ROOT_RT   ge-11/1/4.200         flood           427
0x4480/17 ALT_ROOT_RT   xe-10/0/0.200         flood           427
0x4380/17 ALT_ROOT_RT   xe-10/2/0.200         flood           427

show bridge flood brief

user@host> show bridge flood brief

Name    Active CEs  Active VEs
__juniper_private1__ 0 0
vs1::vlan100        6 0
vs1::vlan200        5 0

show bridge flood detail

user@host> show bridge flood detail

Name: __juniper_private1__
CEs: 0
VEs: 0
```
Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x36/16</td>
<td>MLP_FLOOD</td>
<td><strong>vs1+vlan100</strong></td>
<td>flood</td>
<td>426</td>
</tr>
<tr>
<td>0x3a/16</td>
<td>MLP_FLOOD</td>
<td><strong>vs1+vlan200</strong></td>
<td>flood</td>
<td>428</td>
</tr>
</tbody>
</table>

Name: vs1::vlan100
CEs: 6
VEs: 0

Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35/16</td>
<td>ALL_FLOOD</td>
<td><strong>vs1+vlan100</strong></td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x35/16</td>
<td>RE_FLOOD</td>
<td><strong>vs1+vlan100</strong></td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3780/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/0/3.0</td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3b80/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/4.100</td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3c80/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/1.100</td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3d80/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/0.100</td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3e80/17</td>
<td>ALT_ROOT_RT</td>
<td>xe-10/2/0.100</td>
<td>flood</td>
<td>425</td>
</tr>
<tr>
<td>0x3f80/17</td>
<td>ALT_ROOT_RT</td>
<td>xe-10/0/0.100</td>
<td>flood</td>
<td>425</td>
</tr>
</tbody>
</table>

Name: vs1::vlan200
CEs: 5
VEs: 0

Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x39/16</td>
<td>ALL_FLOOD</td>
<td><strong>vs1+vlan200</strong></td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x39/16</td>
<td>RE_FLOOD</td>
<td><strong>vs1+vlan200</strong></td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x4180/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/0.200</td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x4080/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/1.200</td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x4280/17</td>
<td>ALT_ROOT_RT</td>
<td>ge-11/1/4.200</td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x4480/17</td>
<td>ALT_ROOT_RT</td>
<td>xe-10/0/0.200</td>
<td>flood</td>
<td>427</td>
</tr>
<tr>
<td>0x4380/17</td>
<td>ALT_ROOT_RT</td>
<td>xe-10/2/0.200</td>
<td>flood</td>
<td>427</td>
</tr>
</tbody>
</table>

user@host> show bridge flood extensive

Name: __juniper_private1__
CEs: 0
VEs: 0

Flood route prefix: 0x36/16
Flood route type: MLP_FLOOD
Flood route owner: __vs1+vlan100__
Nexthop type: flood
Nexthop index: 426
Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>lc-11/0/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lc-10/2/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lc-10/0/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lc-11/1/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x3a/16
Flood route type: MLP_FLOOD
Flood route owner: __vs1+vlan200__
Nexthop type: flood
Nexthop index: 428
Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>lc-10/0/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lc-10/2/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lc-11/1/0.32769</td>
<td>LC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood route prefix: 0x35/16</td>
<td>Flood route type: ALL_FLOOD</td>
<td>Flood route owner: <strong>vs1+vlan100</strong></td>
<td>Nexthop type: flood</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------</td>
<td>------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Interfaces Flooding to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flood route prefix: 0x35/16</th>
<th>Flood route type: RE_FLOOD</th>
<th>Flood route owner: <strong>vs1+vlan100</strong></th>
<th>Nexthop type: flood</th>
<th>Nexthop index: 425</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces Flooding to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flood route prefix: 0x3780/17</th>
<th>Flood route type: ALT_ROOT_RT</th>
<th>Flood route owner: ge-11/0/3.0</th>
<th>Nexthop type: flood</th>
<th>Nexthop index: 425</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces Flooding to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flood route prefix: 0x3b80/17</th>
<th>Flood route type: ALT_ROOT_RT</th>
<th>Flood route owner: ge-11/1/4.100</th>
<th>Nexthop type: flood</th>
<th>Nexthop index: 425</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces Flooding to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flood route prefix: 0x3c80/17</th>
<th>Flood route type:</th>
<th>Flood route owner:</th>
<th>Nexthop type:</th>
<th>Nexthop index:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces Flooding to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>NhType</td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>--------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x3d80/17

Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x3e80/17

Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x3f80/17

Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/0/3.0</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x39/16

Name: vs1::vlan200

CEs: 5

VES: 0

Flood route type: ALL_FLOOD
Flood route owner: __vs1+vlan200__
Nexthop type: flood
Nexthop index: 427

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x39/16
Flood route type: RE_FLOOD
Flood route owner: __vs1+vlan200__
Nexthop type: flood
Nexthop index: 427

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x4180/17
Flood route type: ALT_ROOT_RT
Flood route owner: ge-11/1/0.200
Nexthop type: flood
Nexthop index: 427

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x4080/17
Flood route type: ALT_ROOT_RT
Flood route owner: ge-11/1/1.200
Nexthop type: flood
Nexthop index: 427

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x4280/17
Flood route type: ALT_ROOT_RT
Flood route owner: ge-11/1/4.200
Nexthop type: flood
Nexthop index: 427

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Flood route prefix: 0x4480/17
Flood route type: ALT_ROOT_RT
Flood route owner: xe-10/0/0.200
Nexthop type: flood
Nexthop index: 427

Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flood route prefix: 0x4380/17
Flood route type: ALT_ROOT_RT
Flood route owner: xe-10/2/0.200
Nexthop type: flood
Nexthop index: 427

Interfaces Flooding to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>NhType</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>CE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show bridge mac-table**

**Syntax**

```plaintext
show bridge mac-table
  <age>
  <brief | count | detail | extensive>
  <bridge-domain (all | bridge-domain-name)>
  <global-count>
  <instance instance-name>
  <interface interface-name>
  <mac-address>
  <instance instance-name>
  <vlan-id (all-vlan | vlan-id)>
```

**Release Information**

- Command introduced in Junos OS Release 8.4.
- Command introduced in Junos OS Release 15.1
- Support for PBB-EVPN instance added in Junos OS Release 16.1
- MAC Flag P to indicate a MAC Pinned interface introduced in Junos OS 16.2

**Description**

(MX Series routers only) Display Layer 2 MAC address information.

**Options**

- **none**—Display all learned Layer 2 MAC address information.
- **age**—(Optional) Display age of a single mac-address.
- **brief | count | detail | extensive**—(Optional) Display the specified level of output.
- **bridge-domain (all | bridge-domain-name)**—(Optional) Display learned Layer 2 MAC addresses for all bridging domains or for the specified bridging domain.
- **global-count**—(Optional) Display the total number of learned Layer 2 MAC addresses on the system.
- **instance instance-name**—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.
- **interface interface-name**—(Optional) Display learned Layer 2 MAC addresses for the specified interface.
- **mac-address**—(Optional) Display the specified learned Layer 2 MAC address information.
- **vlan-id (all-vlan | vlan-id)**—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

**Additional Information**

When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.
Required Privilege
Level
view

List of Sample Output
show bridge mac-table on page 2572
show bridge mac-table (with Layer 2 Services over GRE Interfaces) on page 2572
show bridge mac-table (with VXLAN enabled) on page 2573
show bridge mac-table age (for GE interface) on page 2573
show bridge mac-table age (for AE interface) on page 2573
show bridge mac-table count on page 2573
show bridge mac-table detail on page 2574
show bridge mac-table instance pbb-evpn on page 2574
show bridge mac-table on page 2574

Output Fields
Table 204 on page 2571 describes the output fields for the `show bridge mac-table` command. Output fields are listed in the approximate order in which they appear.

Table 204: show bridge mac-table Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of a single mac-address.</td>
</tr>
<tr>
<td>Routing instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Bridging domain</td>
<td>Name of the bridging domain.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address or addresses learned on a logical interface.</td>
</tr>
<tr>
<td>MAC flags</td>
<td>Status of MAC address learning properties for each interface:</td>
</tr>
<tr>
<td></td>
<td>• S—Static MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• D—Dynamic MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• L—Locally learned MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• C—Control MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• SE—MAC accounting is enabled.</td>
</tr>
<tr>
<td></td>
<td>• NM—Non-configured MAC.</td>
</tr>
<tr>
<td></td>
<td>• R—Remote PE MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• P—MAC Pinned interface is configured.</td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>MAC count</td>
<td>Number of MAC addresses learned on the specific routing instance or interface.</td>
</tr>
<tr>
<td>Learning interface</td>
<td>Name of the logical interface on which the MAC address was learned.</td>
</tr>
<tr>
<td>Learning VLAN</td>
<td>VLAN ID of the routing instance or bridge domain in which the MAC address was learned.</td>
</tr>
<tr>
<td>VXLAN ID/VXLAN</td>
<td>VXLAN Network Identifier (VNI).</td>
</tr>
</tbody>
</table>
### Table 204: show bridge mac-table Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 flags</td>
<td>Debugging flags signifying that the MAC address is present in various lists.</td>
</tr>
<tr>
<td>Epoch</td>
<td>Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Sequence number assigned to this MAC address. Used for debugging.</td>
</tr>
<tr>
<td>Learning mask</td>
<td>Mask of the Packet Forwarding Engines where this MAC address was learned. Used for debugging.</td>
</tr>
<tr>
<td>IPC generation</td>
<td>Creation time of the logical interface when this MAC address was learned. Used for debugging.</td>
</tr>
</tbody>
</table>

### Sample Output

**show bridge mac-table**

```
user@host> show bridge mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
Bridging domain : test1, VLAN : 1

<table>
<thead>
<tr>
<th>MAC</th>
<th>MAC flags</th>
<th>Logical</th>
<th>NH</th>
<th>RTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:00:0c:cc:cc:cc</td>
<td>S,NM</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00:0c:cc:cc:cd</td>
<td>S,NM</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:00:0c:cd:cd:d0</td>
<td>S,NM</td>
<td>NULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64:87:88:6a:17:d0</td>
<td>D</td>
<td>ae0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64:87:88:6a:17:f0</td>
<td>D</td>
<td>ae0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**show bridge mac-table (with Layer 2 Services over GRE Interfaces)**

```
user@host> show bridge mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
Bridging domain : vlan-1, VLAN : 1

<table>
<thead>
<tr>
<th>MAC</th>
<th>MAC flags</th>
<th>Logical</th>
<th>NH</th>
<th>RTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:01:00:01:f7</td>
<td>D,SE</td>
<td>gr-1/2/10.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:03:00:32:01:f7</td>
<td>D,SE</td>
<td>gr-1/2/10.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:21:11:11:10</td>
<td>DL</td>
<td>ge-1/0/0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:21:11:11:11</td>
<td>DL</td>
<td>ge-1/0/0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Routing instance : default-switch
Bridging domain : vlan-2, VLAN : 2

<table>
<thead>
<tr>
<th>MAC</th>
<th>Logical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show bridge mac-table

user@host> show bridge mac-table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - Statistics enabled, NM - Non configured MAC, R - Remote PE MAC)

Routing instance : default-switch
Bridging domain : vlan-1, VLAN : 1
VXLAN: Id : 100, Multicast group: 233.252.0.1

<table>
<thead>
<tr>
<th>MAC address</th>
<th>flags</th>
<th>interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:01:33:01:f7</td>
<td>D,SE</td>
<td>gr-1/2/10.1</td>
</tr>
<tr>
<td>00:00:21:11:21:10</td>
<td>DL</td>
<td>ge-1/0/0.1</td>
</tr>
<tr>
<td>00:00:21:11:21:11</td>
<td>DL</td>
<td>ge-1/1/0.1</td>
</tr>
</tbody>
</table>

Routing instance : default-switch
Bridging domain : vlan-2, VLAN : 2, VXLAN : 200
VXLAN: Id : 200, Multicast group: 233.252.0.2

<table>
<thead>
<tr>
<th>MAC address</th>
<th>flags</th>
<th>interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:02:01:33:01:f7</td>
<td>D,SE</td>
<td>vtep.1052010</td>
</tr>
<tr>
<td>00:04:00:14:01:f7</td>
<td>D,SE</td>
<td>vtep.1052011</td>
</tr>
<tr>
<td>00:00:21:11:21:10</td>
<td>DL</td>
<td>ge-1/0/0.1</td>
</tr>
<tr>
<td>00:00:21:11:21:11</td>
<td>DL</td>
<td>ge-1/1/0.1</td>
</tr>
</tbody>
</table>

show bridge mac-table age

user@host> show vpls mac-table age 00:02:03:aa:bb:1a instance vpls_instance_1

MAC Entry Age information
Current Age: 4 seconds

show bridge mac-table count

user@host> show bridge mac-table count

2 MAC address learned in routing instance vs1 bridge domain vlan100

MAC address count per interface within routing instance:

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/1/4.100</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/3.0</td>
<td>1</td>
</tr>
</tbody>
</table>
MAC address count per learn VLAN within routing instance:

<table>
<thead>
<tr>
<th>Learn VLAN ID</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

0 MAC address learned in routing instance vs1 bridge domain vlan200

MAC address count per interface within routing instance:

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/0.200</td>
<td>0</td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>0</td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>0</td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>0</td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>0</td>
</tr>
</tbody>
</table>

MAC address count per learn VLAN within routing instance:

<table>
<thead>
<tr>
<th>Learn VLAN ID</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show bridge mac-table detail

user@host> show bridge mac-table detail
MAC address: 00:00:00:19:1c:db
Routing instance: vs1
Bridging domain: vlan100
Learning interface: ge-11/0/3.0 Learning VLAN: 0
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 4 Sequence number: 0
Learning mask: 0x800 IPC generation: 0

MAC address: 00:00:00:59:3a:2f
Routing instance: vs1
Bridging domain: vlan100
Learning interface: xe-10/2/0.100 Learning VLAN: 0
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 7 Sequence number: 0
Learning mask: 0x400 IPC generation: 0

show bridge mac-table instance pbb-evpn

user@host> show bridge mac-table instance pbb-evpn
Routing instance : pbb-evpn
Bridging domain : isid-bd10000, ISID : 10000
<table>
<thead>
<tr>
<th>MAC address</th>
<th>MAC</th>
<th>Logical</th>
<th>NH</th>
<th>RTR</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:19:e2:b0:76:eb</td>
<td>D</td>
<td>cbp.1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>aa:bb:cc:dd:ee:f2</td>
<td>DC</td>
<td></td>
<td>1048576</td>
<td>1048576</td>
</tr>
<tr>
<td>aa:bb:cc:dd:ee:f3</td>
<td>DC</td>
<td></td>
<td>1048575</td>
<td>1048575</td>
</tr>
</tbody>
</table>

show bridge mac-table

user@host>run show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC, O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC, P -Pinned MAC)

Routing instance : VS-541
Bridging domain : 541, VLAN : 541
MAC MAC Logical NH RTR
address flags interface Index ID
00:00:01:00:00:01 D P RC xe-0/0/3.0
00:00:02:00:00:01 D P xe-0/0/3.0
show bridge statistics

Syntax

    show bridge statistics
    <bridge-domain domain-name>
    <instance instance-name>

Release Information

Command introduced in Junos OS Release 8.4.

Description

(MX Series routers only) Display bridge statistics.

Options

    none—Display bridge statistics for all bridge domains in all routing instances.

    bridge-domain domain-name—(Optional) Display statistics for the specified bridge domain.

    instance instance-name—(Optional) Display statistics for the specified routing instance.

Required Privilege

view

List of Sample Output

show bridge statistics on page 2576

Sample Output

show bridge statistics

user@host> show bridge statistics

Information for routing instance:

Routing instance : __juniper_private1__
    Index: 1                        Sequence number: 0
    MAC limit: 5000                 MACs learned: 0
    Static MACs learned: 0          Non config Static MACs learned: 0
    Handle: 0x829e800

Information for routing instance:

Routing instance : vs1
    Bridging domain : vlan100
    Index: 3                        Sequence number: 0
    MAC limit: 5120                 MACs learned: 2
    Static MACs learned: 0          Non config Static MACs learned: 0
    Handle: 0x829e400
    Flags: Bridge instance, Config defined, VLAN : 100
    Local interface: ge-11/0/3.0, Index: 79
    Broadcast packets: 1
    Broadcast bytes : 65
    Multicast packets: 0
    Multicast bytes : 0
    Flooded packets : 0
    Flooded bytes : 0
    Unicast packets : 358624489
<table>
<thead>
<tr>
<th>Local interface</th>
<th>Unicast packets</th>
<th>Unicast bytes</th>
<th>Broadcast packets</th>
<th>Broadcast bytes</th>
<th>Multicast packets</th>
<th>Multicast bytes</th>
<th>Flooded packets</th>
<th>Flooded bytes</th>
<th>Unicast packets</th>
<th>Unicast bytes</th>
<th>Current MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/1/4.100, Index: 84</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 (Limit 1024)</td>
</tr>
<tr>
<td>ge-11/1/1.100, Index: 86</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (Limit 1024)</td>
</tr>
<tr>
<td>ge-11/1/0.100, Index: 87</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (Limit 1024)</td>
</tr>
<tr>
<td>xe-10/2/0.100, Index: 88</td>
<td>358627393</td>
<td>23310781065</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 (Limit 1024)</td>
</tr>
<tr>
<td>xe-10/0/0.100, Index: 89</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (Limit 1024)</td>
</tr>
</tbody>
</table>

Information for routing instance:

Routing instance : vs1
Bridging domain : vlan200

Index: 4                      Sequence number: 0
MAC limit: 5120                MACs learned: 0
Static MACs learned: 0         Non config Static MACs learned: 0
<table>
<thead>
<tr>
<th>Handle: 0x829e600</th>
<th>Flags: Bridge instance, Config defined, VLAN : 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local interface: ge-11/1/0.200, Index: 90</td>
<td></td>
</tr>
<tr>
<td>Broadcast packets:</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast bytes :</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets:</td>
<td>0</td>
</tr>
<tr>
<td>Multicast bytes :</td>
<td>0</td>
</tr>
<tr>
<td>Flooded packets :</td>
<td>0</td>
</tr>
<tr>
<td>Flooded bytes :</td>
<td>0</td>
</tr>
<tr>
<td>Unicast packets :</td>
<td>0</td>
</tr>
<tr>
<td>Unicast bytes :</td>
<td>0</td>
</tr>
<tr>
<td>Current MAC count:</td>
<td>0 (Limit 1024)</td>
</tr>
</tbody>
</table>

| Local interface: ge-11/1/1.200, Index: 91 | 
| Broadcast packets: | 0 |
| Broadcast bytes : | 0 |
| Multicast packets: | 0 |
| Multicast bytes : | 0 |
| Flooded packets : | 0 |
| Flooded bytes : | 0 |
| Unicast packets : | 0 |
| Unicast bytes : | 0 |
| Current MAC count: | 0 (Limit 1024) |

| Local interface: ge-11/1/4.200, Index: 92 | 
| Broadcast packets: | 0 |
| Broadcast bytes : | 0 |
| Multicast packets: | 0 |
| Multicast bytes : | 0 |
| Flooded packets : | 0 |
| Flooded bytes : | 0 |
| Unicast packets : | 0 |
| Unicast bytes : | 0 |
| Current MAC count: | 0 (Limit 1024) |

| Local interface: xe-10/0/0.200, Index: 93 | 
| Broadcast packets: | 0 |
| Broadcast bytes : | 0 |
| Multicast packets: | 0 |
| Multicast bytes : | 0 |
| Flooded packets : | 0 |
| Flooded bytes : | 0 |
| Unicast packets : | 0 |
| Unicast bytes : | 0 |
| Current MAC count: | 0 (Limit 1024) |

| Local interface: xe-10/2/0.200, Index: 94 | 
| Broadcast packets: | 4 |
| Broadcast bytes : | 260 |
| Multicast packets: | 0 |
| Multicast bytes : | 0 |
| Flooded packets : | 0 |
| Flooded bytes : | 0 |
| Unicast packets : | 0 |
| Unicast bytes : | 0 |
| Current MAC count: | 0 (Limit 1024) |
show l2-learning global-information

Syntax  show l2-learning global-information

Release Information  Command introduced in Junos OS Release 8.4.

Description  (MX Series routers only) Display Layer 2 learning process-related information for the entire router.

Options  This command has no options.

Required Privilege Level  view

List of Sample Output  show l2-learning global-information on page 2579

Output Fields  Table 205 on page 2579 describes the output fields for the show l2-learning global-information command. Output fields are listed in the approximate order in which they appear.

Table 205: show l2-learning global-information Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC aging interval</td>
<td>Configured timeout interval, in seconds, for all MAC table entries.</td>
</tr>
<tr>
<td>MAC learning</td>
<td>Status of MAC learning: Enabled or Disabled.</td>
</tr>
<tr>
<td>MAC statistics</td>
<td>Status of MAC accounting: Enabled or Disabled.</td>
</tr>
<tr>
<td>MAC limit Count</td>
<td>Configured maximum limit on the number of MAC addresses that can be learned.</td>
</tr>
<tr>
<td>MAC limit hit flag</td>
<td>Status of the learned MAC limit hit flag: Enabled (the learned MAC exceeds the global MAC limit) or Disabled (the learned MAC does not exceed the global MAC limit).</td>
</tr>
<tr>
<td>MAC packet action drop</td>
<td>Status of action to drop packets after the configured MAC address limit is reached: Enabled (packets are dropped) or Disabled (packets are forwarded).</td>
</tr>
</tbody>
</table>

Sample Output

show l2-learning global-information

user@host> show l2-learning global-information

Global Configuration:
<table>
<thead>
<tr>
<th>MAC aging interval</th>
<th>300</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC learning</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC statistics</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC limit Count</td>
<td>393215</td>
</tr>
<tr>
<td>MAC limit hit flag</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC packet action drop</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
**show l2-learning global-mac-count**

**Syntax**

`show l2-learning global-mac-count`

**Release Information**

Command introduced in Junos OS Release 9.3.

**Description**

(MX Series routers only) Display the total number of dynamic and static MAC addresses learned for the entire router.

**Options**

This command has no options.

**Required Privilege Level**

`view`

**List of Sample Output**

`show l2-learning global-mac-count on page 2581`

**Output Fields**

Displays the total number of dynamic and static MAC addresses learned for the entire router.

**Sample Output**

```
user@host> show l2-learning global-mac-count
100 dynamic and static MAC addresses learned globally
```
show l2-learning instance

Syntax

show l2-learning instance

Release Information

(MX Series routers only) Command introduced in Junos OS Release 8.4.

Description

Display Layer 2 learning properties for all the configured routing instances.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show l2-learning instance on page 2583

Output Fields

Table 206 on page 2582 describes the output fields for the show l2-learning instance command. Output fields are listed in the approximate order in which they appear.

Table 206: show l2-learning instance Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing instance</td>
<td>Name of routing instance.</td>
</tr>
<tr>
<td>Bridging Domain</td>
<td>Name of bridging domain.</td>
</tr>
<tr>
<td></td>
<td>On MX Series routers you can use the show l2-learning instance &lt;extensive&gt; command option to display the Bridge Service-id information which includes the Config Service ID and the Active Service ID.</td>
</tr>
<tr>
<td>Index</td>
<td>Number associated with the routing instance or bridging domain.</td>
</tr>
<tr>
<td>Logical System</td>
<td>Name of logical system or Default if no logical system is configured.</td>
</tr>
<tr>
<td>Routing instance flags</td>
<td>Status of Layer 2 learning properties for each routing instance:</td>
</tr>
<tr>
<td></td>
<td>• DL—MAC learning is disabled.</td>
</tr>
<tr>
<td></td>
<td>• SE—MAC accounting is enabled.</td>
</tr>
<tr>
<td></td>
<td>• AD—Packets are dropped after MAC address limit is reached.</td>
</tr>
<tr>
<td></td>
<td>• LH—The maximum number of MAC addresses has been learned on the routing instance. The routing instance is not able to learn any additional MAC addresses.</td>
</tr>
<tr>
<td>MAC limit</td>
<td>Maximum number of MAC addresses that can be learned from each interface in the routing instance or bridging domain.</td>
</tr>
</tbody>
</table>
Sample Output

`show l2-learning instance`

```bash
user@host> show l2-learning instance

Information for routing instance:

Routing Instance flags (DL - disable learning, SE - stats enabled, AD - packet action drop, LH - mac limit hit)

<table>
<thead>
<tr>
<th>Routing Instance</th>
<th>Bridging Domain</th>
<th>Index</th>
<th>Logical System</th>
<th>Routing flags</th>
<th>MAC limit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>juniper_private1</strong></td>
<td></td>
<td>1</td>
<td>Default</td>
<td></td>
<td>5000</td>
</tr>
<tr>
<td>vs1</td>
<td>vlan100</td>
<td>3</td>
<td>Default</td>
<td></td>
<td>5120</td>
</tr>
<tr>
<td>vs1</td>
<td>vlan200</td>
<td>4</td>
<td>Default</td>
<td></td>
<td>5120</td>
</tr>
</tbody>
</table>

```
show l2-learning interface

Syntax  show l2-learning interface

Release Information  Command introduced in Junos OS Release 8.4. Added sample output to indicate an EVPN MAC Pinned interface, introduced in Junos OS 16.2R1.

Description  (MX Series routers only) Display Layer 2 learning information for all the interfaces.

Options  This command has no options.

Required Privilege Level  view

List of Sample Output  show l2-learning interface on page 2584
show l2-learning-interface on page 2585

Output Fields  Table 207 on page 2584 describes the output fields for the show l2-learning interface command. Output fields are listed in the approximate order in which they appear.

Table 207: show l2-learning interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>Index</td>
<td>Index of the interface.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Number of the routing instance to which the interface belongs.</td>
</tr>
<tr>
<td>Interface device</td>
<td>Value of the order in which the Junos OS finds and initializes the interface.</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>• SE—MAC accounting is enabled.</td>
</tr>
<tr>
<td></td>
<td>• AD—Packets are dropped after the MAC interface limit is reached.</td>
</tr>
<tr>
<td></td>
<td>• MAC limit—Maximum number of MAC addresses that can be learned from the interface.</td>
</tr>
<tr>
<td></td>
<td>• MP—MAC Pinning enabled.</td>
</tr>
</tbody>
</table>

Sample Output

show l2-learning interface

user@host> show l2-learning interface
Information for interface family:

Logical Interface flags (DL - disable learning, SE - stats enabled, AD - packet action drop, LH - mac limit hit)

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Index</th>
<th>Routing instance</th>
<th>Interface device</th>
<th>Logical Interface flags</th>
<th>MAC limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/0/3.0</td>
<td>79</td>
<td>3</td>
<td>136</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/4.100</td>
<td>84</td>
<td>3</td>
<td>150</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/1.100</td>
<td>86</td>
<td>3</td>
<td>147</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/0.100</td>
<td>87</td>
<td>3</td>
<td>146</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>xe-10/2/0.100</td>
<td>88</td>
<td>3</td>
<td>144</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>xe-10/0/0.100</td>
<td>89</td>
<td>3</td>
<td>129</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/0.200</td>
<td>90</td>
<td>4</td>
<td>146</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/1.200</td>
<td>91</td>
<td>4</td>
<td>147</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>ge-11/1/4.200</td>
<td>92</td>
<td>4</td>
<td>150</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>xe-10/0/0.200</td>
<td>93</td>
<td>4</td>
<td>129</td>
<td></td>
<td>1024</td>
</tr>
<tr>
<td>xe-10/2/0.200</td>
<td>94</td>
<td>4</td>
<td>144</td>
<td></td>
<td>1024</td>
</tr>
</tbody>
</table>

show l2 learning-interface

user@host> run show l2-learning interface

Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - Interface Down, MP - MAC Pinning)

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>BD Name Limit</th>
<th>STP State</th>
<th>Logical Interface flags</th>
<th>MP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae0.0</td>
<td>3</td>
<td>0</td>
<td>8192</td>
<td></td>
</tr>
</tbody>
</table>
show mac-rewrite interface

Syntax

```
show mac-rewrite interface
  <brief | detail>
  <interface-name>
```

Release Information

Command introduced in Junos OS Release 9.1.
Command introduced in Junos OS Release 14.1X53-D10 and 17.3R1 for EX4300 switches.
Command introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Command introduced in Junos OS Release 17.4R1 for EX4600 switches.
Statement introduced in Junos OS Release 19.1R1 for QFX5200 switches.

Description

Display Layer 2 protocol tunneling (L2PT) information.

Options

```
brief | detail—(Optional) Display the specified level of output.

interface interface-name—(Optional) Display L2PT information for the specified interface.
```

Required Privilege Level

view

Related Documentation

- `layer2-control`
- `mac-rewrite`
- `protocol`
- `Understanding Layer 2 Protocol Tunneling`
- `Configuring Layer 2 Protocol Tunneling`

List of Sample Output

show mac-rewrite interface on page 2587
show mac-rewrite interface (EX Series Switches) on page 2587

Output Fields

Table 208 on page 2586 lists the output fields for the `show mac-rewrite interface` command. Output fields are listed in the approximate order in which they appear.

**Table 208: show mac-rewrite 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>Name of the interface on which L2PT is configured.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 208: show mac-rewrite 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>Protocols</td>
<td>Layer 2 protocols being tunneled on this interface.</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>All devices that support L2PT can tunnel the following protocols: Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following Layer 2 protocols can also be tunneled on some devices that support L2PT: E-LMI, GVRP, IEEE 802.1X, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, PVSTP+, UDLD, or VSTP. See protocol for more information on the supported protocols for tunneling on different devices.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show mac-rewrite interface

```
user@host> show mac-rewrite interface
Interface       Protocols
ge-1/0/5       STP VTP CDP PVSTP+
```

show mac-rewrite interface (EX Series Switches)

```
user@switch> show mac-rewrite interface
Interface       Protocols
ge-0/0/1       802.3AH LLDP STP
```
CHAPTER 30

VPN Operational Commands

• clear vpls mac-address
• clear vpls mac-table
• request l2circuit-switchover
• show dynamic-tunnels database
• show hfr profiles
• show ingress-replication mvpn
• show l2circuit connections
• show l2vpn connections
• show mvpn c-multicast
• show mvpn instance
• show mvpn neighbor
• show vpls connections
• show vpls flood event-queue
• show vpls flood instance
• show vpls flood route
• show vpls mac-table
• show vpls statistics
clear vpls mac-address

Syntax

```
clear vpls mac-address
<instance instance-name >
<logical-system (all | logical-system-name)>
<mac-address>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(T Series and M Series routers, except for the M160 router) Clear media access control (MAC) address entries from the virtual private LAN service (VPLS) table.

Options

- **none**—Clear all MAC address entries from the VPLS table for all routing instances.
- **instance instance-name**—(Optional) Clear all MAC address entries for a VPLS instance from the VPLS table.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **mac-address**—(Optional) Clear a specific MAC address in a VPLS instance from the VPLS table.

Required Privilege Level

maintenance

List of Sample Output

clear vpls mac-address on page 2590

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear vpls mac-address

```
user@host> clear vpls mac-address
```
clear vplsl mac-table

**Syntax**
clear vplsmac-table
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
<mac-address>
<vlan-id>

**Release Information**
Command introduced before Junos OS Release 9.5.

**Description**
(MX Series routers) Clear media access control (MAC) addresses from the virtual private LAN service (VPLS) MAC table.

**Options**
- **none**—Clear all MAC addresses from the VPLS table for all routing instances.
- **instance instance-name**—(Optional) Clear all MAC addresses for a VPLS instance from the VPLS table.
- **interface interface-name**—(Optional) Clear all MAC addresses for a VPLS interface from the VPLS table.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **mac-address**—(Optional) Clear a specific MAC address in a VPLS instance from the VPLS table.
- **vlan-id**—(Optional) Clear MAC addresses on a specified VLAN (0 through 4095).

**Required Privilege Level**
maintenance

**List of Sample Output**
clear vplsmac-table on page 2591

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear vplsmac-table

user@host> clear vplsmac-table
request l2circuit-switchover

Syntax
request l2circuit-switchover
<logical-system (all | logical-system-name)>
<neighbor address>
<virtual-circuit-id identifier>

Release Information
Command introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series and for EX4600 switches.

Description
Manually trigger a switch from the active pseudowire to the redundant pseudowire. This command can be useful when performing network maintenance.

Options
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
neighbor address—(Optional) Trigger a switch of all of the active pseudowire connections with the specified neighbor to their respective redundant pseudowires.
virtual-circuit-id identifier—(Optional) Trigger a switch from the active pseudowire connection of the specified Layer 2 circuit to its redundant pseudowire.

Required Privilege
maintenance

Related Documentation
- MPLS Feature Support on QFX Series and EX4600 Switches

List of Sample Output
request l2circuit-switchover virtual-circuit-id on page 2592

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request l2circuit-switchover virtual-circuit-id

user@host>request l2circuit-switchover virtual-circuit-id 12
show dynamic-tunnels database

Syntax

show dynamic-tunnels database
<destination>
<logical-system (all | logical-system-name)>
<table routing-table-name>

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display dynamic tunnel database information.

Options

none—Display dynamic tunnel database information for all destinations and routing tables.

destination—(Optional) Display database entries for the specified IP address (with optional destination prefix length) only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

table routing-table-name—(Optional) Display database entries for the specified table only.

Required Privilege

view

List of Sample Output

show dynamic-tunnels database (Tunnel Is Up) on page 2594
show dynamic-tunnels database (No Tunnel PIC) on page 2595
show dynamic-tunnels database (Tunnel Is Expiring) on page 2595
show dynamic-tunnels database (Destination Specified) on page 2595
show dynamic-tunnels database (Localization) on page 2595
show dynamic-tunnels database (MPLS-over-UDP Dynamic Tunnels on PTX Series Routers and QFX Series Switches) on page 2596
show dynamic-tunnels database (Segment Routing LSPs) on page 2596

Output Fields

Table 209 on page 2593 lists the output fields for the show dynamic-tunnels database command. Output fields are listed in the approximate order in which they appear.

Table 209: show dynamic-tunnels database Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>Destination-network</td>
<td>Destination IP address and subnet.</td>
</tr>
<tr>
<td>Tunnel to</td>
<td>Destination IP address and prefix of the tunnel.</td>
</tr>
</tbody>
</table>
Table 209: show dynamic-tunnels database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the tunnel: Up, Up (expires in nn:nn:nn seconds), or Dn (down).</td>
</tr>
<tr>
<td>Reference count</td>
<td>Number of routes across the dynamic tunnel that are currently being resolved.</td>
</tr>
</tbody>
</table>
| Next-hop type | Type of tunnel: GRE or UDP (BGP-Signal).  
  • GRE or UDP (BGP signal)  
  • SRTE—Segment routing traffic-engineered LSP. |
| Source address | Source IP address of the tunnel. |
| Next-hop     | IP address of the destination interface. |
| VPN Label    | The label provided by the peer device to identify the VPN through which the packet needs to go. This label is used to identify the VRF for route lookup. |
| Ingress Route | The IGP route along with the corresponding metric that has been selected for forwarding the tunnel-encapsulated packet. |
| Localized PFE | Packet Forwarding Engine interface which is the anchor Packet Forwarding Engine for the localized next-hop-based dynamic tunnels.  
  When the anchor Packet Forwarding Engine of the tunnel goes down, it is represented by a # near the Packet Forwarding Engine name. |
| LSP template name | Name of the segment routing traffic-engineered template configured for dynamic creation of segment routing LSPs. |
| State         | State of the destination interface: Up, Dn, or Dn (no tunnel pic). |
| Status        | Status of the dynamic segment routing LSP. |

Sample Output

show dynamic-tunnels database (Tunnel Is Up)

```
user@host> show dynamic-tunnels database
Table: inet.3
Destination-network: 10.255.120.94/32
Tunnel to: 10.255.120.94/32
  Reference count: 4
  Next-hop type: UDP
    Source address: 10.255.120.92
    Next hop: tunnel-composite, 0x31132f64, nhid 3406
    VPN Label: Push 120 Reference count: 3
    Ingress Route: 10.255.120.94/32, via metric 2
```
show dynamic-tunnels database (No Tunnel PIC)

```
user@host> show dynamic-tunnels database
Table: inet.3

Destination-network: 10.255.120.94/32
Tunnel to: 10.255.120.94/32 State: Dn
   Reference count: 2
   Next-hop type: gre
   Source address: 10.255.120.92
   State: Dn (no tunnel pic)
```

show dynamic-tunnels database (Tunnel Is Expiring)

```
user@host> show dynamic-tunnels database
Table: inet.3

Destination-network: 10.255.120.94/32
Tunnel to: 10.255.120.94/32 State: Up (expires in 00:14:56 seconds)
   Reference count: 0
   Next-hop type: gre
   Source address: 10.255.120.92
   Next hop: gr-4/3/0.32769
   State: Up
```

show dynamic-tunnels database (Destination Specified)

```
user@host> show dynamic-tunnels database 10.255.120.94
Table: inet.3

Destination-network: 10.255.120.94/32
Tunnel to: 10.255.120.94/32 State: Up
   Reference count: 2
   Next-hop type: gre
   Source address: 10.255.120.92
   Next hop: gr-4/3/0.32769
   State: Up
```

show dynamic-tunnels database (Localization)

```
user@host> show dynamic-tunnels database
Destination-network: 1.0.0.0/8
Tunnel to: 1.1.1.6/32
   Reference count: 5
   Next-hop type: UDP
   Source address: 1.1.1.2
   Next hop: tunnel-composite, 0xc807930, nhid 1016
   Localized PFE: pfe-1/0/0
   VPN Label: Push 299808 Reference count: 4
   Ingress Route: 1.1.1.6/32, via metric 2
   Traffic Statistics: Packets 0, Bytes 0
   State: Up
```
show dynamic-tunnels database (MPLS-over-UDP Dynamic Tunnels on PTX Series Routers and QFX Series Switches)

user@host>  show dynamic-tunnels database
  *- Signal Tunnels #- PFE-down
  Table: inet.3
  Destination-network: 22.33.0.0/16
  Destination-network: 22.33.44.0/24

show dynamic-tunnels database (Segment Routing LSPs)

user@host>  show dynamic-tunnels database
  Table: inetcolor.0
  Destination-network: 22.33.44.0/0/24
  Tunnel to: 22.33.44.55:124/64
  Reference count: 2
  Next-hop type: SRTE
  LSP template name: 22.33.44.55:7c:dt-srte-tunnel1
  Status: Initiated/Established
show hfr profiles

Syntax

```
show hfr profiles
<brief | extensive>
```

Release Information

Command introduced in Junos OS Release 12.2.

Description

Display host fast reroute (HFRR) profile information.

HFRR adds a precomputed protection path into the Packet Forwarding Engine, such that if a link between a provider edge device and a server farm becomes unusable for forwarding, the Packet Forwarding Engine can use another path without having to wait for the router or the protocols to provide updated forwarding information.

Options

- none—Display information about HFRR profiles.
- brief | extensive—(Optional) Display the specified level of output.

Required Privilege

view

Related Documentation

- Example: Configuring Link Protection with Host Fast Reroute

List of Sample Output

```
show hfr profiles on page 2598
```

Output Fields

Table 210 on page 2597 describes the output fields for the `show hfr profiles` command. Output fields are listed in the approximate order in which they appear.

Table 210: show hfr profiles Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFRR</td>
<td></td>
</tr>
<tr>
<td>HFRR current state</td>
<td>Status of the HFRR profile: HFRR_ACTIVE, HFRR_INACTIVE, HFRR_IFLH-NOT-CONF, and so on.</td>
</tr>
<tr>
<td>HFRR Prefix limit blackout timer expiry (in secs)</td>
<td>Time interval between an HFRR profile becoming inactive on exceeding the ARP prefix limit, and the profile starting the SYNC process.</td>
</tr>
<tr>
<td>HFRR prefix limit hit count</td>
<td>Number of times that an HFRR profile becomes inactive on exceeding the ARP prefix limit.</td>
</tr>
<tr>
<td>HFRR protected IFL name</td>
<td>Interface configured for the HFRR feature.</td>
</tr>
<tr>
<td>HFRR protected IFL handle</td>
<td></td>
</tr>
</tbody>
</table>
### Table 210: show hfrr profiles Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFRR routing instance name</td>
<td>The routing instance in which the HFRR interface is configured.</td>
</tr>
<tr>
<td>HFRR routing instance handle</td>
<td></td>
</tr>
<tr>
<td>HFRR sync BG scheduled</td>
<td></td>
</tr>
<tr>
<td>HFRR RTS filter on</td>
<td></td>
</tr>
<tr>
<td>HFRR delete BG scheduled</td>
<td></td>
</tr>
<tr>
<td>HFRR ARP prefix limit</td>
<td>Configured ARP prefix limit.</td>
</tr>
<tr>
<td>HFRR ARP supplementary blackout timeout (in mins)</td>
<td>Supplementary time-out value configured for profile to be inactive when it hits ARP prefix limit.</td>
</tr>
<tr>
<td>HFRR number of ARP routes learned</td>
<td>Number of ARP routes learned on the configured interface.</td>
</tr>
<tr>
<td>HFRR number of FRR routes created</td>
<td>Number of ARP routes created on the configured interface.</td>
</tr>
</tbody>
</table>

### Sample Output

```
user@host> show hfrr profiles
HFRR pointer: 0x9254000
HFRR current state: HFRR_ACTIVE
HFRR Prefix limit blackout timer expiry (in secs): 0
HFRR prefix limit hit count: 0
HFRR protected IFL name: ge-4/1/0.0
HFRR protected IFL handle: 0x9248738
HFRR routing instance name: test
HFRR routing instance handle: 0x9145740
HFRR sync BG scheduled: NO
HFRR RTS filter on: YES
HFRR delete BG scheduled: NO
HFRR ARP prefix limit: 0
HFRR ARP supplementary blackout timeout (in mins): 1
HFRR number of ARP routes learned: 4
HFRR number of FRR routes created: 2
```
show ingress-replication mvpn

Syntax
show ingress-replication mvpn

Release Information
Command introduced in Junos OS Release 10.4.

Description
Display the state and configuration of the ingress replication tunnels created for the MVPN application when using the mpls-internet-multicast routing instance type.

Required Privilege
View

List of Sample Output
show ingress-replication mvpn on page 2599

Output Fields
Table 211 on page 2599 lists the output fields for the show ingress-replication mvpn 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>Ingress tunnel</td>
<td>Identifies the MVPN ingress replication tunnel.</td>
</tr>
<tr>
<td>Application</td>
<td>Identifies the application (MVPN).</td>
</tr>
<tr>
<td>Unicast tunnels</td>
<td>List of unicast tunnels in use.</td>
</tr>
<tr>
<td>Leaf address</td>
<td>Address of the tunnel.</td>
</tr>
<tr>
<td>Tunnel type</td>
<td>Identifies the unicast tunnel type.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates whether the tunnel was created as a new tunnel for the ingress replication, or if an existing tunnel was used.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the tunnel is Up or Down.</td>
</tr>
</tbody>
</table>

Sample Output

show ingress-replication mvpn

```
user@host> show ingress-replication mvpn

Ingress Tunnel: mvpn:1
Application: MVPN
Unicast tunnels
Leaf Address       Tunnel-type       Mode       State
10.255.245.2       P2P LSP           New        Up
10.255.245.4       P2P LSP           New        Up

Ingress Tunnel: mvpn:2
Application: MVPN
```
<table>
<thead>
<tr>
<th>Leaf Address</th>
<th>Tunnel-type</th>
<th>Mode</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.245.2</td>
<td>P2P LSP</td>
<td>Existing</td>
<td>Up</td>
</tr>
</tbody>
</table>
show l2circuit connections

Syntax show l2circuit connections
<br/>&lt;brief | extensive | summary&gt;
<br/>&lt;down | up | up-down&gt;
<br/>&lt;history&gt;
<br/>&lt;interface interface-name&gt;
<br/>&lt;logical-system (all | logical-system-name)&gt;
<br/>&lt;neighbor neighbor&gt;
<br/>&lt;status&gt;

Release Information Command introduced before Junos OS Release 7.4.
Display enhancements in Junos OS Release 10.2.
Display enhancements in Junos OS Release 12.1.
Display enhancements in Junos OS Release 13.2.
Statement introduced in Junos OS Release 14.1X53-D10 for the QFX Series and for EX4600 switches.

Description Display status information about Layer 2 virtual circuits from the local provider edge (PE) router to its neighbors.

Options none—Display standard information about Layer 2 virtual circuits on all interfaces for all neighbors.

brief | extensive | summary—(Optional) Display the specified level of output. Use history to display information about connection history. Use status to display information about the connection and interface status.

down | up | up-down—(Optional) Display nonoperational, operational, or both kinds of connections.

history—(Optional) Display information about connection history.

interface interface-name—(Optional) Show all Layer 2 virtual circuits on an interface.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor neighbor—(Optional) IP address of a specific neighbor.

status—(Optional) Display information about the connection and interface status.

Required Privilege Level view

List of Sample Output show l2circuit connections on page 2605
show l2circuit connections interface on page 2606
show l2circuit connections extensive on page 2606
show l2circuit connections extensive (Pseudowire Redundancy with Hot Standby) on page 2607

Output Fields

Table 212 on page 2602 lists the output fields for the show l2circuit connections command. Output fields are listed in the approximate order in which they appear.

Table 212: show l2circuit connections Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer-2 Circuit Connections</td>
<td>Displays the legends for connection and interface status.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Remote PE neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Logical PE-to-CE interface on which the virtual circuit is configured.</td>
</tr>
<tr>
<td>Type</td>
<td>VC type: rmt (remote) or loc (local).</td>
</tr>
</tbody>
</table>
### Table 212: `show l2circuit connections` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Legend for connection status (St)</strong></td>
<td>Status of the virtual circuit connection:</td>
</tr>
<tr>
<td>EI</td>
<td>The local virtual circuit interface is configured with an encapsulation that is not supported.</td>
</tr>
<tr>
<td>MM</td>
<td>The two routers do not agree on an MTU value, which causes an MTU mismatch.</td>
</tr>
<tr>
<td>EM</td>
<td>The encapsulation type received on this virtual circuit from the neighbor does not match the local virtual circuit interface encapsulation type.</td>
</tr>
<tr>
<td>CM</td>
<td>The two routers do not agree on a control word, which causes a control word mismatch.</td>
</tr>
<tr>
<td>VM</td>
<td>The remote and local VLAN IDs do not match across the Layer 2 circuit.</td>
</tr>
<tr>
<td>OL</td>
<td>No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.</td>
</tr>
<tr>
<td>NC</td>
<td>The interface is not configured as a CCC or TCC interface.</td>
</tr>
<tr>
<td>BK</td>
<td>The virtual circuit has switched to a backup connection.</td>
</tr>
<tr>
<td>CB</td>
<td>The remote PE router is advertising a different cell bundle from that configured on the local PE router.</td>
</tr>
<tr>
<td>LD</td>
<td>The connection to the local site is signaled down, because the CE-facing interface to the local site is down.</td>
</tr>
<tr>
<td>RD</td>
<td>The remote neighbor is down. It has signaled a problem using the pseudowire status code.</td>
</tr>
<tr>
<td>NP</td>
<td>The router detects that interface hardware is not present. The hardware may be offline, a PIC may not be of the desired type, or the interface may be configured in a different routing instance.</td>
</tr>
<tr>
<td>Dn</td>
<td>The virtual circuit is down.</td>
</tr>
<tr>
<td>VC-Dn</td>
<td>The virtual circuit is down because there is no tunnel LSP from the local PE router to the neighbor.</td>
</tr>
<tr>
<td>UP</td>
<td>The virtual circuit is operational.</td>
</tr>
<tr>
<td>CF</td>
<td>The router cannot find enough bandwidth to the remote router to satisfy the Layer 2 circuit bandwidth requirement.</td>
</tr>
<tr>
<td>IB</td>
<td>The bit rate is incompatible for Time Division Multiplexing (TDM).</td>
</tr>
<tr>
<td>TDM</td>
<td>TDM is not configured correctly.</td>
</tr>
<tr>
<td>ST</td>
<td>The virtual circuit has been switched to a standby connection.</td>
</tr>
<tr>
<td>SP</td>
<td>The virtual circuit connection is using a static pseudowire.</td>
</tr>
<tr>
<td>RS</td>
<td>The remote site is in a standby state.</td>
</tr>
<tr>
<td>XX</td>
<td>The virtual circuit is down for an unknown reason. This is a programming error.</td>
</tr>
</tbody>
</table>

| **Time last up** | Date and time the virtual circuit was last operational. |
| **# Up trans** | Number of times the virtual circuit came up. |
| **local-interface-name** | Name of the local PE-to-CE interface. |
| **Status** | Status of the local interface. |
| **Up** | Interface is operational. |
Table 212: show l2circuit connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dn</td>
<td>Interface is not operational.</td>
</tr>
<tr>
<td>NP</td>
<td>Not present. Interface does not exist.</td>
</tr>
<tr>
<td>DS</td>
<td>Disabled. Interface has been administratively disabled.</td>
</tr>
<tr>
<td>WE</td>
<td>Wrong encapsulation. The interface is not configured as CCC.</td>
</tr>
<tr>
<td>UN</td>
<td>Interface status is initialized.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation of the local interface.</td>
</tr>
<tr>
<td>Flow Label Transmit</td>
<td>Flow label transmit status.</td>
</tr>
<tr>
<td>Flow Label Receive</td>
<td>Flow label receive status.</td>
</tr>
<tr>
<td>Remote PE</td>
<td>Prefix of the remote PE router.</td>
</tr>
<tr>
<td>Negotiated control-word</td>
<td>Whether the use of the control word has been negotiated for this virtual circuit: Yes (Null) or No.</td>
</tr>
<tr>
<td>Incoming label</td>
<td>Label used by the remote side of the virtual circuit to send packets destined to the local side. This label is routed to the local virtual circuit interface.</td>
</tr>
<tr>
<td>Outgoing label</td>
<td>Label used by the local side of the virtual circuit to send packets to the remote side of the virtual circuit. Packets originated on the local virtual circuit interface are encapsulated with this label before being placed on the tunnel LSP to the neighbor for this virtual circuit. This label is allocated by the neighbor and is used in demultiplexing incoming packets destined for this virtual circuit.</td>
</tr>
<tr>
<td>Negotiated PW status TLV</td>
<td>Displays the pseudowire status type, length, and value (TLV). TLVs are a method of encoding variable-length or optional information. If the pseudowire status TLV is used, the corresponding local or neighbor PE router status code is also displayed.</td>
</tr>
<tr>
<td>local PW status code</td>
<td>If the pseudowire status TLV is used, displays the local PE router status code.</td>
</tr>
<tr>
<td>Neighbor PW status code</td>
<td>If the pseudowire status TLV is used, displays the neighbor PE router status code.</td>
</tr>
<tr>
<td>Local interface</td>
<td>Name of the local interface used for the Layer 2 circuit connection.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the local interface (Up or Down).</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation configured for the local interface.</td>
</tr>
<tr>
<td>APS-active</td>
<td>Indicates that the interface belongs to the working circuit.</td>
</tr>
</tbody>
</table>
Table 212: `show l2circuit connections` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APS-inactive</td>
<td>Indicates that the interface belongs to the protect circuit.</td>
</tr>
<tr>
<td>Connection protection</td>
<td>Whether or not connection protection is configured for the Layer 2 circuit to the neighbor: Yes or No.</td>
</tr>
<tr>
<td>VC bandwidth</td>
<td>Bandwidth requirement of the Layer 2 circuit.</td>
</tr>
<tr>
<td>Time</td>
<td>Time at which the event occurred.</td>
</tr>
<tr>
<td>Connection History</td>
<td>Event types logged in history.</td>
</tr>
<tr>
<td></td>
<td>• <code>loc intf up</code>—Local virtual circuit interface went up.</td>
</tr>
<tr>
<td></td>
<td>• <code>loc intf down</code>—Local virtual circuit interface went down.</td>
</tr>
<tr>
<td></td>
<td>• <code>in lbl Update</code>—Incoming label has been updated.</td>
</tr>
<tr>
<td></td>
<td>• <code>out lbl Update</code>—Outgoing label has been updated.</td>
</tr>
<tr>
<td></td>
<td>• <code>PE route changed</code>—Route to PE router has been updated.</td>
</tr>
<tr>
<td></td>
<td>• <code>PE route down</code>—Route to PE router is down.</td>
</tr>
<tr>
<td></td>
<td>• <code>rmt side marked</code>—Remote side is marked.</td>
</tr>
<tr>
<td></td>
<td>• <code>VC Dn</code>—Remote side indicated that its end of the virtual circuit is down (if the tunnel LSP from the remote side to the local side is down).</td>
</tr>
<tr>
<td></td>
<td>• <code>status update timer</code>—Status update timer processing. It computes the state of the virtual circuit, and determines whether it should be advertised to or withdrawn from the remote side.</td>
</tr>
</tbody>
</table>

Sample Output

`show l2circuit connections`

`user@host> show l2circuit connections`

Layer-2 Circuit Connections:

Legend for connection status (St)
- EI -- encapsulation invalid
- MM -- mtu mismatch
- EM -- encapsulation mismatch
- CM -- control-word mismatch
- VM -- vlan id mismatch
- OL -- no outgoing label
- NC -- intf encaps not CCC/TCC
- BK -- Backup Connection
- CB -- rcvd cell-bundle size bad
- LD -- local site signaled down
- RD -- remote site signaled down
- XX -- unknown

Legend for interface status
- Up -- operational
- Dn -- down

Neighbor: 10.255.245.51

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

show l2circuitconnectionsinterface

user@host> show l2circuitconnectionsinterface t1-2/0/0:1:1.0

Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid      NP -- interface h/w not present
MM -- mtu mismatch              DN -- down
EM -- encapsulation mismatch    VC-Dn -- Virtual circuit Down
CM -- control-word mismatch     Up -- operational
VM -- vlan id mismatch          CF -- Call admission control failure
OL -- no outgoing label         IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC   TM -- TDM misconfiguration
BK -- Backup Connection         ST -- Standby Connection
LD -- local site signaled down  SP -- Static Pseudowire
RD -- remote site signaled down HS -- hot standby
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down

Neighbor: 10.1.1.1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>t1-2/0/0:1:1.0(vc 1)(SP)</td>
<td>rmt Up</td>
<td>Dec 7 18:11:18 2009</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Remote PE: 10.255.245.51, Negotiated control-word: No
Incoming label: 299856, Outgoing label: 299808
Negotiated PW status TLV: No
Local interface: ge-2/0/2.600, Status: Up, Encapsulation: VLAN
Flow Label Transmit: No, Flow Label Receive: No
Auto-sensed or Programmed by XYZ

Sample Output

show l2circuitconnections extensive

user@host> show l2circuitconnections extensive

Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid      NP -- interface h/w not present
MM -- mtu mismatch              DN -- down
EM -- encapsulation mismatch    VC-Dn -- Virtual circuit Down
CM -- control-word mismatch     Up -- operational
VM -- vlan id mismatch          CF -- Call admission control failure
OL -- no outgoing label         IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC   TM -- TDM misconfiguration
BK -- Backup Connection         ST -- Standby Connection
LD -- local site signaled down  SP -- Static Pseudowire
RD -- remote site signaled down HS -- hot standby
XX -- unknown
Sample Output

show l2circuit connections extensive (Pseudowire Redundancy with Hot Standby)

user@host> show l2circuit connections extensive

Layer-2 Circuit Connections:

Legend for connection status (St)
EI -- encapsulation invalid
MM -- mtu mismatch
EM -- encapsulation mismatch
CM -- control-word mismatch
VM -- vlan id mismatch
OL -- no outgoing label
NC -- intf encaps not CCC/TCC
BK -- Backup Connection
CB -- rcvd cell-bundle size bad
LD -- local site signaled down
RD -- remote site signaled down
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down

Neighbor: 192.0.2.101

Interface       Type  St     Time last up          # Up trans
ge-1/3/2.600(vc 1)        rmt   Up     Jan 24 11:00:26 2013           1
Remote PE: 192.0.2.101, Negotiated control-word: Yes (Null)
Incoming label: 299776, Outgoing label: 299776
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN
Connection History:
2607
Jan 24 11:00:26 2013  status update timer
Jan 24 11:00:26 2013  PE route changed
Jan 24 11:00:26 2013  Out lbl Update                    299776
Jan 24 11:00:26 2013  In lbl Update                     299776
Jan 24 11:00:26 2013  loc intf up                 ge-1/3/2.600

Neighbor: 192.0.2.102

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/3/2.600(vc 2)</td>
<td>rmt</td>
<td>HS</td>
<td>-----</td>
<td>----</td>
</tr>
</tbody>
</table>

Remote PE: 192.0.2.102, Negotiated control-word: Yes (Null)
Incoming label: 299792, Outgoing label: 299776
Negotiated PW status TLV: Yes
Local PW status code: 0x000000020, Neighbor PW status code: 0x00000000
Local interface: ge-1/3/2.600, Status: Up, Encapsulation: VLAN
show l2vpn connections

Syntax

```show l2vpn connections
<brief | extensive>
<down | up | up-down>
<history>
<instance instance>
<instance-history>
<local-site local-site>
<logical-system (all | logical-system-name)>
<remote-site remote-site>
<status>
<summary>
```

Release Information
Command introduced before Junos OS Release 7.4.
`instance-history` option introduced in Junos OS Release 12.3R2.

Description
Display Layer 2 virtual private network (VPN) connections.

Options
- `none`—Display all Layer 2 VPN connections for all routing instances.
- `brief | extensive`—(Optional) Display the specified level of output.
- `down | up | up-down`—(Optional) Display nonoperational, operational, or both kinds of connections.
- `history`—(Optional) Display information about connection history.
- `instance instance`—(Optional) Display connections for the specified routing instance only.
- `instance-history`—(Optional) Display information about connection history for a particular instance.
- `local-site local-site`—(Optional) Display connections for the specified Layer 2 VPN local site name or ID only.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `remote-site remote-site`—(Optional) Display connection for the specified Layer 2 VPN remote site ID only.
- `status`—(Optional) Display information about the connection and interface status.
- `summary`—(Optional) Display summary of all Layer 2 VPN connections information.

Required Privilege
- Level `view`
List of Sample Output

- show l2vpn connections on page 2612
- show l2vpn connections on page 2613
- show l2vpn connections extensive on page 2614
- show l2vpn connections extensive (VPWS) on page 2614

Output Fields

Table 213 on page 2610 lists the output fields for the `show l2vpn connections` command. Output fields are listed in the approximate order in which they appear.

Table 213: show l2vpn connections Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of Layer 2 VPN instance.</td>
</tr>
<tr>
<td>L2vpn-id</td>
<td>For BGP autodiscovery, a globally unique Layer 2 VPN community identifier for the instance.</td>
</tr>
<tr>
<td>Local-ID</td>
<td>BGP <code>local-address</code> assigned to the local routing device.</td>
</tr>
<tr>
<td>Local site</td>
<td>Name of local site.</td>
</tr>
<tr>
<td>Local source-attachment-id</td>
<td>For FEC 129, the VPWS source attachment identifier. The point-to-point nature of VPWS requires that you specify the source access individual identifier (SAII) and the target access individual identifier (TAII). This SAII-TAII pair defines a unique pseudowire between two PE devices.</td>
</tr>
<tr>
<td>Target-attachment-id</td>
<td>For FEC 129, the VPWS target attachment identifier. If the configured target identifier matches a source identifier advertised by a remote PE device by way of a BGP auto-discovery message, the pseudowire between that source-target pair is signaled. If there is no match between an advertised source identifier and the configured target identifier, the pseudowire is not established.</td>
</tr>
<tr>
<td>Interface name</td>
<td>Name of interface.</td>
</tr>
<tr>
<td>Remote Site ID</td>
<td>Remote site ID.</td>
</tr>
<tr>
<td>Label Offset</td>
<td>Numbers within the label block that are skipped to find the next label base.</td>
</tr>
<tr>
<td>Label-base</td>
<td>Advertises the first label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.</td>
</tr>
<tr>
<td>Range</td>
<td>Advertises the label block size.</td>
</tr>
<tr>
<td>status-vector</td>
<td>Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of 0 indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of 1 indicates either one or both are down.</td>
</tr>
<tr>
<td>connection-site</td>
<td>Name of the connection site.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of connection: <code>loc</code> (local) or <code>rmt</code> (remote).</td>
</tr>
<tr>
<td>St</td>
<td>Status of the connection. (For a list of possible values, see the Legend for connection status (St) field.)</td>
</tr>
</tbody>
</table>
### Table 213: show l2vpn connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time last up</td>
<td>Time that the connection was last in the Up condition.</td>
</tr>
<tr>
<td># Up trans</td>
<td>Number of transitions from Down to Up condition.</td>
</tr>
<tr>
<td>Local circuit</td>
<td>Address and status of local circuit.</td>
</tr>
<tr>
<td>Remote circuit</td>
<td>Address and status of remote circuit.</td>
</tr>
</tbody>
</table>

**St**

Status of the Layer 2 VPN connection (corresponds with Legend for Connection Status):

- **EI**—The local Layer 2 VPN interface is configured with an encapsulation that is not supported.
- **EM**—The encapsulation type received on this Layer 2 VPN connection from the neighbor does not match the local Layer 2 VPN connection interface encapsulation type.
- **VC-Dn**—The virtual circuit is currently down.
- **CM**—The two routers do not agree on a control word, which causes a control word mismatch.
- **CN**—The virtual circuit is not provisioned properly.
- **OR**—The label associated with the virtual circuit is out of range.
- **OL**—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.
- **LD**—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established.
- **RD**—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established.
- **LN**—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site.
- **RN**—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site.
- **XX**—The Layer 2 VPN connection is down for an unn reason. This is a programming error.
- **NC**—The interface encapsulation is not configured as an appropriate CCC, TCC, or Layer 2 VPN encapsulation.
- **WE**—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the Layer 2 VPN routing instance.
- **NP**—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance.
- **->**—Only the outbound connection is up.
- **<--**—Only the inbound connection is up.
- **Up**—The Layer 2 VPN connection is operational.
- **Dn**—The Layer 2 VPN connection is down.
- **CF**—The router cannot find enough bandwidth to the remote router to satisfy the Layer 2 VPN connection bandwidth requirement.
### Table 213: `show l2vpn connections` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SC</strong></td>
<td>The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers.</td>
</tr>
<tr>
<td><strong>LM</strong></td>
<td>The local site identifier is not the minimum designated, meaning it is not the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site, and the associated local site identifier is not being used to distribute Layer 2 VPN label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state.</td>
</tr>
<tr>
<td><strong>RM</strong></td>
<td>The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state.</td>
</tr>
<tr>
<td><strong>IL</strong></td>
<td>The incoming packets for the Layer 2 VPN connection have no MPLS label.</td>
</tr>
<tr>
<td>Remote PE</td>
<td>Address of the remote provider edge router.</td>
</tr>
<tr>
<td>Incoming label</td>
<td>Name of the incoming label.</td>
</tr>
<tr>
<td>Outgoing label</td>
<td>Name of the outgoing label.</td>
</tr>
<tr>
<td>Egress Protection</td>
<td>Whether the given PVC is protected by connection protection logic using egress protection for BGP signaled layer 2 services.</td>
</tr>
<tr>
<td>Flow Label Receive</td>
<td>Capability to pop the flow label in the receive direction to the remote provider edge (PE) router</td>
</tr>
<tr>
<td>Flow Label Transmit</td>
<td>Capability to push the flow label in the transmit direction to the provider edge (PE) router</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of Layer 2 VPN connection event.</td>
</tr>
<tr>
<td>Event</td>
<td>Type of event.</td>
</tr>
<tr>
<td>Interface/Lbl/PE</td>
<td>Interface, label, or PE router.</td>
</tr>
</tbody>
</table>

### Sample Output

`show l2vpn connections`

```
user@host> show l2vpn connections
L2VPN Connections:
Instance: vpn1
Edge protection: Not-Primary
Local site: 2 (ce-2)
```
### show l2vpn connections

#### Layer-2 VPN connections:

Legend for connection status (St):
- EI -- encapsulation invalid
- EM -- encapsulation mismatch
- VC-Dn -- Virtual circuit down
- CM -- control-word mismatch
- CN -- circuit not provisioned
- OR -- out of range
- OL -- no outgoing label
- LD -- local site signaled down
- RD -- remote site signaled down
- LN -- local site not designated
- RN -- remote site not designated
- XX -- unknown connection status
- MM -- MTU mismatch
- BK -- Backup connection
- PF -- Profile parse failure
- RS -- remote site standby
- LB -- Local site not best-site
- VM -- VLAN ID mismatch

Legend for interface status:
- Up -- operational
- Dn -- down

Instance: l2vpn-inst

Edge protection: Not-Primary

Local site: pe2 (2)

<table>
<thead>
<tr>
<th>connection-site</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>rmt</td>
<td>Up</td>
<td>Jun 22 14:46:50 2015</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote PE: 10.255.255.1, Negotiated control-word: Yes (Null)
Incoming label: 800002, Outgoing label: 800003
Local interface: ge-0/0/1.300, Status: Up, Encapsulation: VLAN
Flow Label Transmit: Yes, Flow Label Receive: Yes
show l2vpn connections extensive

user@host> show l2vpn connections extensive

L2VPN Connections:
Instance: vpn-a
Edge protection: Not-Primary
Local site: ce-a (1)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Remote Site ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/0.0</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label Offset</th>
<th>Offset</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

connection-site: Type St Time last up # Up trans
2 rmt Up Aug 3 00:08:14 2001 1

Local circuit: fe-0/0/0.0, Status: Up
Remote PE: 192.168.24.1
Incoming label: 32769, Outgoing label: 32768
Egress Protection: Yes

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Interface/Lbl/PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 3 00:08:14 2001</td>
<td>PE route up</td>
<td></td>
</tr>
<tr>
<td>Aug 3 00:08:14 2001</td>
<td>Out lbl Update</td>
<td>32768</td>
</tr>
<tr>
<td>Aug 3 00:08:14 2001</td>
<td>In lbl Update</td>
<td>32769</td>
</tr>
<tr>
<td>Aug 3 00:08:14 2001</td>
<td>ckt0 up</td>
<td></td>
</tr>
</tbody>
</table>

show l2vpn connections extensive (VPWS)

user@host> show l2vpn connections

Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid
EM -- encapsulation mismatch
VC-Dn -- Virtual circuit down
CM -- control-word mismatch
CN -- circuit not provisioned
OR -- out of range
OL -- no outgoing label
LD -- local site signaled down
RD -- remote site signaled down
LN -- local site not designated
RN -- remote site not designated
XX -- unknown connection status

Legend for interface status
Up -- operational
Dn -- down

Instance: FEC129-VPWS
L2vpn-id: 100:100
Number of local interfaces: 1
Number of local interfaces up: 1
ge-2/0/5.0
Local source-attachment-id: 1 (ONE)
<table>
<thead>
<tr>
<th>Target-attachment-id</th>
<th>Type</th>
<th>St</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>rmt</td>
<td>Up</td>
<td>Nov 28 16:16:14 2012</td>
<td>1</td>
</tr>
</tbody>
</table>

Remote PE: 198.51.100.2, Negotiated control-word: No
Incoming label: 299792, Outgoing label: 299792
Local interface: ge-2/0/5.0, Status: Up, Encapsulation: ETHERNET

Connection History:
- Nov 28 16:16:14 2012 status update timer
- Nov 28 16:16:14 2012 PE route changed
- Nov 28 16:16:14 2012 Out lbl Update 299792
- Nov 28 16:16:14 2012 In lbl Update 299792
- Nov 28 16:16:14 2012 loc intf up ge-2/0/5.0
show mvnp c-multicast

Syntax
show mvnp c-multicast
  <extensive | summary>  
  <instance-name instance-name>
  <source-pe>

Release Information
Command introduced in Junos OS Release 8.4.
Option to show source-pe introduced in Junos OS Release 15.1.

Description
Display the multicast VPN customer multicast route information.

Options
extensive | summary—(Optional) Display the specified level of output.
instance-name instance-name—(Optional) Display output for the specified routing instance.
source-pe—(Optional) Display source-pe output for the specified c-multicast entries.

Required Privilege
view

List of Sample Output
show mvnp c-multicast on page 2617
show mvnp c-multicast summary on page 2617
show mvnp c-multicast extensive on page 2617
show mvnp c-multicast source-pe on page 2618

Output Fields
Table 214 on page 2616 lists the output fields for the show mvnp c-multicast command. Output fields are listed in the approximate order in which they appear.

Table 214: show mvnp c-multicast Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the VPN routing instance.</td>
<td>summary extensive none</td>
</tr>
<tr>
<td>C-mcast IPv4 (S,G)</td>
<td>Customer router IPv4 multicast address.</td>
<td>extensive none</td>
</tr>
<tr>
<td>Ptnl</td>
<td>Provider tunnel attributes, tunnel type:tunnel source, tunnel destination group.</td>
<td>extensive none</td>
</tr>
<tr>
<td>St</td>
<td>State:</td>
<td>extensive none</td>
</tr>
<tr>
<td>MVVPN instance</td>
<td>Name of the multicast VPN routing instance</td>
<td>extensive none</td>
</tr>
</tbody>
</table>
Table 214: show mvpn c-multicast Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-multicast IPv4</td>
<td>Number of customer multicast IPv4 routes associated with the multicast VPN</td>
<td>summary</td>
</tr>
<tr>
<td>route count</td>
<td>routing instance.</td>
<td></td>
</tr>
<tr>
<td>C-multicast IPv6</td>
<td>Number of customer multicast IPv6 routes associated with the multicast VPN</td>
<td>summary</td>
</tr>
<tr>
<td>route count</td>
<td>routing instance.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show mvpn c-multicast

user@host> show mvpn c-multicast

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel  S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)  RM -- remote VPN route

Instance: VPN-A
C-mcast IPv4 (S:G)  Ptnl  St

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel  S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)  RM -- remote VPN route

Instance: VPN-B
C-mcast IPv4 (S:G)  Ptnl  St
192.168.195.94/32:203.0.113.0/24  PIM-SM:10.255.14.144, 198.51.100.2  RM

show mvpn c-multicast summary

user@host> show mvpn c-multicast summary

MVPN Summary:
Family: INET
Family: INET6

Instance: mvpn1
C-multicast IPv6 route count: 1

show mvpn c-multicast extensive

user@host> show mvpn c-multicast extensive

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel  S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
show mvnpn c-multicast source-pe

user@host> show mvnpn c-multicast source-pe

Family : INET
Family : INET6

Instance : mvpn1
MVPN Mode : RPT-SPT
C-Multicast route address: ::/0:ff05::1/128
  VPN Source-PE1:
    extended-community: no-advertise target:10.1.0.0:9
    Route Distinguisher: 10.1.0.0:1
    Autonomous system number: 1
    Interface: ge-0/0/9.1 Index: 343
  PIM Source-PE1:
    extended-community: target:10.1.0.0:9
    Route Distinguisher: 10.1.0.0:1
    Autonomous system number: 1
    Interface: ge-0/0/9.1 Index: 343
show mvpn instance

Syntax

```
show mvpn instance
<instance-name>
<display-tunnel-name>
<extensive | summary>
<inet | inet6>
<logical-system>
```

Release Information

Command introduced in Junos OS Release 8.4.
Additional details in output for extensive option introduced in Junos OS Release 15.1.

Description

Display the multicast VPN routing instance information according the options specified.

Options

- **instance-name**—(Optional) Display statistics for the specified routing instance, or press Enter without specifying an instance name to show output for all instances.

- **display-tunnel-name**—(Optional) Display the ingress provider tunnel name rather than the attribute.

- **extensive | summary**—(Optional) Display the specified level of output.

- **inet | inet6**—(Optional) Display output for the specified IP type.

- **logical-system**—(Optional) Display details for the specified logical system, or type “all”.

Required Privilege

- **Level** view

List of Sample Output

- show mvpn instance on page 2620
- show mvpn instance summary on page 2621
- show mvpn instance extensive on page 2621
- show mvpn instance summary (IPv6) on page 2622

Output Fields

Table 215 on page 2619 lists the output fields for the *show mvpn instance* 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>MVVPN instance</td>
<td>Name of the multicast VPN routing instance</td>
<td>extensive none</td>
</tr>
<tr>
<td>Instance</td>
<td>Name of the VPN routing instance.</td>
<td>summary extensive none</td>
</tr>
<tr>
<td>Provider tunnel</td>
<td>Provider tunnel attributes, <em>tunnel type:tunnel source, tunnel destination group.</em></td>
<td>extensive none</td>
</tr>
</tbody>
</table>
### Table 215: `show mvpn 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>Neighbor</td>
<td>Address, type of provider tunnel (I-P-tnl, inclusive provider tunnel and S-P-tnl, selective provider tunnel) and provider tunnel for each neighbor.</td>
<td>extensive none</td>
</tr>
<tr>
<td>C-mcast IPv4 (S:G)</td>
<td>Customer IPv4 router multicast address.</td>
<td>extensive none</td>
</tr>
<tr>
<td>C-mcast IPv6 (S:G)</td>
<td>Customer IPv6 router multicast address.</td>
<td>extensive none</td>
</tr>
<tr>
<td>Ptnl</td>
<td>Provider tunnel attributes, <code>tunnel type: tunnel source, tunnel destination group</code>.</td>
<td>extensive none</td>
</tr>
<tr>
<td>St</td>
<td>State:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- DS—Represents (S,G) and is created due to (*,G)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- RM—Remote VPN route learned from the remote PE router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- St display blank—SSM group join</td>
<td></td>
</tr>
<tr>
<td>Neighbor count</td>
<td>Number of neighbors associated with the multicast VPN routing instance.</td>
<td>summary</td>
</tr>
<tr>
<td>C-multicast IPv4 route count</td>
<td>Number of customer multicast IPv4 routes associated with the multicast VPN routing instance.</td>
<td>summary</td>
</tr>
<tr>
<td>C-multicast IPv6 route count</td>
<td>Number of customer multicast IPv6 routes associated with the multicast VPN routing instance.</td>
<td>summary</td>
</tr>
</tbody>
</table>

### Sample Output

```bash
css user@host> show mvpn instance

MVPN instance:

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Provider tunnel: I-P-tnl</th>
<th>I-P-tnl</th>
<th>10.255.14.144, 198.51.100.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Provider tunnel: S-P-tnl</td>
<td>S-P-tnl</td>
<td>10.255.14.160, 198.51.100.1</td>
</tr>
<tr>
<td>Neighbor count</td>
<td></td>
<td>10.255.70.17</td>
<td>PIM-SM:10.255.70.17, 198.51.100.1</td>
</tr>
<tr>
<td>Neighbor count</td>
<td></td>
<td>192.168.195.78/32:203.0.113.0/24</td>
<td>PIM-SM:10.255.14.144, 198.51.100.1</td>
</tr>
</tbody>
</table>

MVPN instance:

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Provider tunnel: I-P-tnl</th>
<th>I-P-tnl</th>
<th>10.255.14.144, 198.51.100.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Provider tunnel: S-P-tnl</td>
<td>S-P-tnl</td>
<td>10.255.14.160, 198.51.100.1</td>
</tr>
<tr>
<td>Neighbor count</td>
<td></td>
<td>10.255.70.17</td>
<td>PIM-SM:10.255.70.17, 198.51.100.1</td>
</tr>
<tr>
<td>Neighbor count</td>
<td></td>
<td>192.168.195.78/32:203.0.113.0/24</td>
<td>PIM-SM:10.255.14.144, 198.51.100.1</td>
</tr>
</tbody>
</table>
```
Sample Output

show mvpn instance summary

```
user@host> show mvpn instance summary
MVPN Summary:
Family: INET
Family: INET6

Instance: mvpn1
Sender-Based RPF: Disabled. Reason: Not enabled by configuration.
Hot Root Standby: Disabled. Reason: Not enabled by configuration.
Neighbor count: 3
C-multicast IPv6 route count: 1
```

Sample Output

show mvpn instance extensive

```
user@host> show mvpn instance extensive
MVPN instance:
Family : INET

Instance : vpn_blue
Customer Source: 10.1.1.1
   RT-Import Target: 192.168.1.1:100
   Route-Distinguisher: 192.168.1.1:100
   Source-AS: 65000
   Via unicast route: 10.1.0.0/16 in vpn-blue.inet.0
   Candidate Source PE Set:
       RT-Import 192.168.1.1:100, RD 1111:22222, Source-AS 65000
       RT-Import 192.168.2.2:100, RD 1111:22222, Source-AS 65000
       RT-Import 192.168.3.3:100, RD 1111:22222, Source-AS 65000

'Extensive' output will show everything in 'detail' output and add the list of bound c-multicast routes.

> show mvpn source 10.1.1.1 instance vpn_blue extensive

Family : INET

Instance : vpn_blue
Customer Source: 10.1.1.1
   RT-Import Target: 192.168.1.1:100
   Route-Distinguisher: 192.168.1.1:100
   Source-AS: 65000
   Via unicast route: 10.1.0.0/16 in vpn-blue.inet.0
   Candidate Source PE Set:
       RT-Import 192.168.1.1:100, RD 1111:22222, Source-AS 65000
```
show mvpn instance summary (IPv6)

user@host> show mvpn instance summary

MVPN Summary:
Instance: VPN-A
  C-multicast IPv6 route count: 2
Instance: VPN-B
  C-multicast IPv6 route count: 2
**show mvpn neighbor**

**Syntax**

```
show mvpn neighbor
  <extensive | summary>
  <inet | inet6>
  <instance instance-name | neighbor-address address>
  <logical-system logical-system-name>
```

**Release Information**

Command introduced in Junos OS Release 8.4.

**Description**

Display multicast VPN neighbor information.

**Options**

- `extensive | summary`—(Optional) Display the specified level of output for all multicast VPN neighbors.
- `inet | inet6`—(Optional) Display IPv4 or IPv6 information for all multicast VPN neighbors.
- `instance instance-name | neighbor-address address`—(Optional) Display multicast VPN neighbor information for the specified instance or the specified neighbor.
- `logical-system logical-system-name`—(Optional) Display multicast VPN neighbor information for the specified logical system.

**Required Privilege**

```
view
```

**List of Sample Output**

- `show mvpn neighbor on page 2624`
- `show mvpn neighbor extensive on page 2624`
- `show mvpn neighbor extensive on page 2625`
- `show mvpn neighbor instance-name on page 2625`
- `show mvpn neighbor neighbor-address on page 2625`
- `show mvpn neighbor neighbor-address summary on page 2626`
- `show mvpn neighbor neighbor-address extensive on page 2626`
- `show mvpn neighbor neighbor-address instance-name on page 2626`
- `show mvpn neighbor summary on page 2627`

**Output Fields**

`Table 216 on page 2623 lists the output fields for the show mvpn neighbor 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>MVPN instance</td>
<td>Name of the multicast VPN routing instance</td>
<td>extensive none</td>
</tr>
<tr>
<td>Instance</td>
<td>Name of the VPN routing instance.</td>
<td>summary extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>

Copyright © 2019, Juniper Networks, Inc.
Table 216: show mvpn neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Address, type of provider tunnel (I-P-tnl, inclusive provider tunnel and S-P-tnl, selective provider tunnel) and provider tunnel for each neighbor.</td>
<td>extensive none</td>
</tr>
<tr>
<td>Provider tunnel</td>
<td>Provider tunnel attributes, <strong>tunnel type:</strong> <strong>tunnel source, tunnel destination group.</strong></td>
<td>extensive none</td>
</tr>
</tbody>
</table>

**Sample Output**

**show mvpn neighbor**

```plaintext
user@host> show mvpn neighbor

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)   RM -- remote VPN route

Instance: VPN-A

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>I-P-tnl</th>
<th>PIM-SM:10.255.14.160, 192.0.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.70.17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Instance: VPN-B

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)   RM -- remote VPN route

Instance: VPN-B

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>I-P-tnl</th>
<th>PIM-SM:10.255.14.160, 192.0.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.70.17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Sample Output**

**show mvpn neighbor extensive**

```plaintext
user@host> show mvpn neighbor extensive

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)   RM -- remote VPN route

Instance: VPN-A

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>I-P-tnl</th>
<th>PIM-SM:10.255.14.160, 192.0.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.70.17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Instance: VPN-B

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)   RM -- remote VPN route

Instance: VPN-B

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>I-P-tnl</th>
<th>PIM-SM:10.255.14.160, 192.0.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.160</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.70.17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show mvpn neighbor extensive

user@host> show mvpn neighbor extensive

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route

Instance: mvpn-a

Neighbor I-P-tnl
10.255.72.45
10.255.72.50 LDP P2MP:10.255.72.50, lsp-id 1

Sample Output

show mvpn neighbor instance-name

user@host> show mvpn neighbor instance-name VPN-A

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route

Instance: VPN-A

Neighbor I-P-tnl
10.255.14.160
10.255.70.17 PIM-SM:10.255.14.160, 192.0.2.1
10.255.70.17 PIM-SM:10.255.70.17, 192.0.2.1

Sample Output

show mvpn neighbor neighbor-address

user@host> show mvpn neighbor neighbor-address 10.255.14.160

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route

Instance: VPN-A
Sample Output

show mvpn neighbor neighbor-address summary

user@host> show mvpn neighbor neighbor-address 10.255.70.17 summary

MVPN Summary:
Instance: VPN-A
Instance: VPN-B

Sample Output

show mvpn neighbor neighbor-address extensive

user@host> show mvpn neighbor neighbor-address 10.255.70.17 extensive

MVPN instance:

Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route

Instance: VPN-A
Neighbor 10.255.70.17 I-P-tnl
PIM-SM:10.255.70.17, 192.0.2.1

Sample Output

show mvpn neighbor neighbor-address instance-name

user@host> show mvpn neighbor neighbor-address 10.255.70.17 instance-name VPN-A

MVPN instance:
Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g) RM -- remote VPN route

Instance: VPN-A
Neighbor 10.255.70.17 I-P-tnl
          PIM-SM:10.255.70.17, 192.0.2.1

Sample Output

show mvpn neighbor summary

user@host> show mvpn neighbor summary

MVPN Summary:
Family: INET
Family: INET6

Instance: mvpn1
Neighbor count: 3
show vpls connections

Syntax

```
show vpls connections
  <brief | extensive>
  <down | up | up-down>
  <history>
  <instance instance-name local-site local-site-name remote-site remote-site-name>
  <instance-history>
  <logical-system (all | logical-system-name)>
  <status>
  <summary>
```

Release Information

Command introduced before Junos OS Release 7.4.

`instance-history` option introduced in Junos OS Release 12.3R2.

Description

(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) connection information.

Options

```
one—Display information about all VPLS connections for all routing instances.
brief | extensive—(Optional) Display the specified level of output.
down | up | up-down—(Optional) Display nonoperational, operational, or both types of connections.
history—(Optional) Display information about connection history.
instance instance-name—(Optional) Display the VPLS connections for the specified routing instance only.
instance-history—(Optional) Display information about connection history for a particular instance.
local-site local-site-name—(Optional) Display the VPLS connections for the specified local site name or ID only.
remote-site remote-site-name—(Optional) Display the VPLS connections for the specified remote site name or ID only. Label block size information is always shown as 0 when using this option.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
status—(Optional) Display information about the connection and interface status.
summary—(Optional) Display summary of all VPLS connections information.
```

Required Privilege

View
List of Sample Output

- `show vpls connections on page 2633`
- `show vpls connections (with FEC128 and FEC129 in the same routing-instance) on page 2635`
- `show vpls connections (with multiple pseudowires) on page 2636`
- `show vpls connections extensive (Static VPLS Neighbors) on page 2637`

Output Fields

Table 217 on page 2629 lists the output fields for the `show vpls connections` command. Output fields are listed in the approximate order in which they appear.

**Table 217: show vpls connections Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the VPLS instance.</td>
</tr>
<tr>
<td>Local site</td>
<td>Name of the local site.</td>
</tr>
<tr>
<td>VPLS-id</td>
<td>Identifier for the VPLS site.</td>
</tr>
<tr>
<td>Number of local interfaces</td>
<td>Number of interfaces configured for the local site.</td>
</tr>
<tr>
<td>Number of local interfaces up</td>
<td>Number of interfaces configured for the local site that are currently up.</td>
</tr>
<tr>
<td>IRB interface present</td>
<td>Indicates whether or not an integrated routing and bridging (IRB) interface is present (yes or no).</td>
</tr>
</tbody>
</table>
| Intf                | List of all of the interfaces configured for the local site. The types of interfaces can include VPLS virtual loopback tunnel interfaces and label-switched interfaces. Any interface that supports VPLS could be listed here. Virtual loopback tunnel interfaces are displayed using the `vt-fpc/pic/port.nnnnn` format. Label-switched interfaces are displayed using the `lsi.nnnnn` format. In both cases, `nnnnn` is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain. Each interface might include the following information:  
  - Identification as a VPLS interface  
  - Name of the associated VPLS routing instance  
  - Local site number  
  - Remote site number  
  - VPLS neighbor address  
  - VPLS identifier  
<table>
<thead>
<tr>
<th>Interface flags</th>
<th>Flag associated with the interface. Can include the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC-Down</td>
<td>The virtual circuit associated with this interface is down.</td>
</tr>
<tr>
<td>Label-base</td>
<td>First label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.</td>
</tr>
</tbody>
</table>
### Table 217: show vpls connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset</td>
<td>Displays the VPLS Edge (VE) block offset in the Layer 2 VPN NLRI. The VE block offset is used to identify a label block from which a particular label value is selected to setup a pseudowire for a remote site. The block offset value itself indicates the starting VE ID that maps to the label base contained in the VPLS NLRI advertisement.</td>
</tr>
<tr>
<td>Size</td>
<td>Label block size. A configurable value that represents the number of label blocks required to cover all the pseudowires for the remote peer. Acceptable configuration values are: 2, 4, 8 and 16. The default value is 2. A value of 0 will be displayed when using the remote-site option.</td>
</tr>
<tr>
<td>Range</td>
<td>Label block range. A value that keeps track of the numbers of remote sites discovered within each label block.</td>
</tr>
<tr>
<td>Preference</td>
<td>Preference value advertised for a VPLS site. When multiple PE routers are assigned the same VE ID for multihoming, you might need to specify that a particular PE router acts as the designated forwarder by configuring the site preference value. The site preference indicates the degree of preference for a particular customer site. The site preference is one of the tie-breaking criteria used in a designated forwarder election.</td>
</tr>
<tr>
<td>status-vector</td>
<td>Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of 0 indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of 1 indicates either one or both are down.</td>
</tr>
<tr>
<td>connection-site</td>
<td>Name of the connection site.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address and VPLS identifier for the VPLS neighbor. If multiple pseudowires have been configured, the IP address will also show the PW-specific vpls-id-list, for example, 203.0.113.144 (vpls-id 200).</td>
</tr>
<tr>
<td>Type</td>
<td>Type of connection: loc (local) or rmt (remote).</td>
</tr>
</tbody>
</table>
### Table 217: `show vpls connections Output Fields (continued)`

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>St</strong></td>
<td>Status of the VPLS connection (corresponds with Legend for Connection Status):</td>
</tr>
<tr>
<td></td>
<td>• EI—The local VPLS interface is configured with an encapsulation that is not supported.</td>
</tr>
<tr>
<td></td>
<td>• EM—The encapsulation type received on this VPLS connection from the neighbor does not match the local VPLS connection interface encapsulation type.</td>
</tr>
<tr>
<td></td>
<td>• VC-Dn—The virtual circuit is currently down.</td>
</tr>
<tr>
<td></td>
<td>• CM—The two routers do not agree on a control word, which causes a control word mismatch.</td>
</tr>
<tr>
<td></td>
<td>• CN—The virtual circuit is not provisioned properly.</td>
</tr>
<tr>
<td></td>
<td>• OR—The label associated with the virtual circuit is out of range.</td>
</tr>
<tr>
<td></td>
<td>• OL—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit.</td>
</tr>
<tr>
<td></td>
<td>• LD—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established.</td>
</tr>
<tr>
<td></td>
<td>• RD—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established.</td>
</tr>
<tr>
<td></td>
<td>• LN—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site.</td>
</tr>
<tr>
<td></td>
<td>• RN—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site.</td>
</tr>
</tbody>
</table>

In a multihoming configuration, one multihomed PE site displays the state **LN**, and the other multihomed PE site displays the state **RN** in the following circumstances:

- The multihomed links are both configured to be the backup site.
- The two multihomed PE routers have the same site ID, but have a peering relationship with a route reflector (RR) that has a different site ID.
- **XX**—The VPLS connection is down for an unreason. This is a programming error.
- **MM**—The MTU for the local site and the remote site do not match.
- **BK**—The router is using a backup connection.
- **PF**—Profile parse failure.
- **RS**—The remote site is in a standby state.
- **NC**—The interface encapsulation is not configured as an appropriate CCC, TCC, or VPLS encapsulation.
- **WE**—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the VPLS routing instance.
Table 217: show vpls connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP</td>
<td>The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance.</td>
</tr>
<tr>
<td>--&gt;</td>
<td>Only the outbound connection is up.</td>
</tr>
<tr>
<td>&lt;--</td>
<td>Only the inbound connection is up.</td>
</tr>
<tr>
<td>Up</td>
<td>The VPLS connection is operational.</td>
</tr>
<tr>
<td>Dn</td>
<td>The VPLS connection is down.</td>
</tr>
<tr>
<td>CF</td>
<td>The router cannot find enough bandwidth to the remote router to satisfy the VPLS connection bandwidth requirement.</td>
</tr>
<tr>
<td>SC</td>
<td>The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers.</td>
</tr>
<tr>
<td>LM</td>
<td>The local site identifier is not the minimum designated, meaning it is not the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site. the associated local site identifier is not being used to distribute VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state.</td>
</tr>
<tr>
<td>RM</td>
<td>The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state.</td>
</tr>
<tr>
<td>IL</td>
<td>The incoming packets for the VPLS connection have no MPLS label.</td>
</tr>
<tr>
<td>MI</td>
<td>The configured mesh group identifier is in use by another system in the network.</td>
</tr>
<tr>
<td>ST</td>
<td>The router has switched to a standby connection.</td>
</tr>
<tr>
<td>PB</td>
<td>Profile busy.</td>
</tr>
<tr>
<td>SN</td>
<td>The VPLS neighbor is static.</td>
</tr>
</tbody>
</table>

**Time last up**  
Time connection was last in the **Up** condition.

**# Up trans**  
Number of transitions from **Down** to **Up** condition.

**Status**  
Status of the (local or remote circuit) local interface:

- **Up**—Operational
- **Dn**—Down
- **NP**—Not present
- **DS**—Disabled
- **WE**—Wrong encapsulation
- **UN**—Uninitialized

**Encapsulation**  
Type of encapsulation: **VPLS**.

**Remote PE**  
Address of the remote provider edge router.
Table 217: show vpls connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negotiated control-word</td>
<td>Whether a control word has been negotiated: Yes or No.</td>
</tr>
<tr>
<td>Incoming label</td>
<td>Name of the incoming label.</td>
</tr>
<tr>
<td>Outgoing label</td>
<td>Name of the outgoing label.</td>
</tr>
<tr>
<td>Negotiated PW status TLV</td>
<td>Indicates whether or not the pseudowire status TLV has been negotiated for the VPLS connection.</td>
</tr>
<tr>
<td>Local interface</td>
<td>Provides the following information about the local interface configured for the VPLS neighbor:</td>
</tr>
<tr>
<td></td>
<td>• Name of the local interface</td>
</tr>
<tr>
<td></td>
<td>• Status—Interface status (Up or Down)</td>
</tr>
<tr>
<td></td>
<td>• Encapsulation—Interface encapsulation (for example, ETHERNET)</td>
</tr>
<tr>
<td></td>
<td>• Description—Includes the VPLS instance name, the VPLS neighbor address, and the VPLS identifier</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of VPLS connection event.</td>
</tr>
<tr>
<td>Event</td>
<td>Type of event.</td>
</tr>
<tr>
<td>Interface/Lbl/PE</td>
<td>Interface, label, or PE router.</td>
</tr>
<tr>
<td>Connection History</td>
<td>Each entry can include the date, time, year, and the connection event. Connection events include any of a variety of events related to VPLS connections, such as route changes, label updates, and interfaces going down or coming up.</td>
</tr>
</tbody>
</table>

Sample Output

show vpls connections

user@host> show vpls connections

Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid       NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      < -- only outbound connection is up
CN -- circuit not provisioned    > -- only inbound connection is up
OR -- out of range              Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unn connection status      IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not available
<table>
<thead>
<tr>
<th>Instance: vpls-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local site: 1 (11)</td>
</tr>
<tr>
<td>Number of local interfaces: 1</td>
</tr>
<tr>
<td>Number of local interfaces up: 1</td>
</tr>
<tr>
<td>IRB interface present: no</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Status</th>
<th>Time last up</th>
<th># Up trans</th>
</tr>
</thead>
<tbody>
<tr>
<td>vt-1/3/0.1048588</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/2/0.1048591</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/2/0.1048585</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/2/0.1048587</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/2/0.1048589</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/3/0.1048586</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/3/0.1048590</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vt-1/3/0.1048584</td>
<td>Intf</td>
<td>vpls vpls-1 local site 11 remote site 8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Label-base Offset Size Range Preference
800256 1 16 16 100

Timer Values:
- Startup wait time: 120 seconds
- New site wait-time: 20 seconds
- Collision detect time: 30 seconds
- Reclaim wait time: 748 milliseconds

Remote PE: 192.0.2.1, Negotiated control-word: No
Incoming label: 800256, Outgoing label: 800026
Local interface: vt-1/3/0.1048588, Status: Up, Encapsulation: VPLS
Description: Intf - vpls vpls-1 local site 11 remote site 1

Connection History:
- Apr 28 13:28:24 2009 status update timer
- Apr 28 13:24:27 2009 status update timer
- Apr 28 13:24:27 2009 loc intf up vt-1/3/0.1048588
- Apr 28 13:24:27 2009 PE route changed
- Apr 28 13:24:27 2009 In lbl Update 800256
- Apr 28 13:24:27 2009 loc intf down

Remote PE: 192.0.2.71, Negotiated control-word: No
Incoming label: 800257, Outgoing label: 800034
Local interface: vt-1/2/0.1048591, Status: Up, Encapsulation: VPLS
Description: Intf - vpls vpls-1 local site 11 remote site 2

Connection History:
- Apr 28 13:28:24 2009 status update timer
- Apr 28 13:24:28 2009 status update timer
show vpls connections (with FEC128 and FEC129 in the same routing-instance)

```
user@host> show vpls connections

Instance: fec129
L2vpn-id: 1:1
Local-id: 203.0.113.0
FEC129-VPLS State:
  Mesh-group connections: __ves__
  Remote-id             Type  St     Time last up          # Up trans
  203.0.3.3             rmt   Up     Sep 19 09:59:56 2017           1
  Remote PE: 203.0.3.3, Negotiated control-word: No
  Incoming label: 262155, Outgoing label: 262164
  Negotiated PW status TLV: No
  Local interface: lsi.1048844, Status: Up, Encapsulation: ETHERNET
  Description: Intf - vpls fec129 local-id 10.4.4.4 remote-id 203.0.3.3
  neighbor 203.0.3.3
  Flow Label Transmit: No, Flow Label Receive: No
  203.0.2.2             rmt   Up     Sep 19 09:59:52 2017           1
  Remote PE: 203.0.2.2, Negotiated control-word: No
  Incoming label: 262154, Outgoing label: 262157
  Negotiated PW status TLV: No
  Local interface: lsi.1048846, Status: Up, Encapsulation: ETHERNET
  Description: Intf - vpls fec129 local-id 10.4.4.4 remote-id 203.0.2.2
  neighbor 203.0.2.2
  Flow Label Transmit: No, Flow Label Receive: No
  203.0.1.1             rmt   Up     Sep 19 09:59:48 2017           1
  Remote PE: 203.0.1.1, Negotiated control-word: No
  Incoming label: 262156, Outgoing label: 262157
  Negotiated PW status TLV: No
  Local interface: lsi.1048845, Status: Up, Encapsulation: ETHERNET
  Description: Intf - vpls fec129 local-id 10.4.4.4 remote-id 203.0.1.1
  neighbor 203.0.1.1
  Flow Label Transmit: No, Flow Label Receive: No

LDP-VPLS State
  Mesh-group connections: MG1
  Neighbor                   Type  St     Time last up          # Up trans
  203.0.6.6(vpls-id 1)      rmt   Up     Sep 17 19:17:11 2017           1
  Remote PE: 203.0.6.6, Negotiated control-word: No
  Incoming label: 262423, Outgoing label: 262145
  Negotiated PW status TLV: No
  Local interface: lsi.1049859, Status: Up, Encapsulation: ETHERNET
  Description: Intf - vpls bgp-vpls neighbor 203.0.6.6 vpls-id 1
  Flow Label Transmit: No, Flow Label Receive: No
  203.0.7.7(vpls-id 1)      rmt   Up     Sep 17 19:17:04 2017           1
  Remote PE: 203.0.7.7, Negotiated control-word: No
  Incoming label: 262424, Outgoing label: 262145
  Negotiated PW status TLV: No
  Local interface: lsi.1049857, Status: Up, Encapsulation: ETHERNET
  Description: Intf - vpls bgp-vpls neighbor 203.0.7.7 vpls-id 1
  Flow Label Transmit: No, Flow Label Receive: No

Mesh-group connections: MG2
  Neighbor                   Type  St     Time last up          # Up trans
```
show vpls connections (with multiple pseudowires)

user@host> show vpls connections

Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down     NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not available
BK -- Backup connection         ST -- Standby connection
PF -- Profile parse failure     PB -- Profile busy
RS -- remote site standby       SN -- Static Neighbor
LB -- Local site not best-site  RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: vpls
VPLS-id: 100
Mesh-group connections: __yes__
Neighbor                  Type  St     Time last up          # Up trans
10.255.114.3 (vpls-id 100)  rmt   Up     Apr 11 23:38:38 2013           1
Remote PE: 10.255.114.3, Negotiated control-word: No
Incoming label: 262145, Outgoing label: 262145
Negotiated PW status TLV: No
Local interface: lsi.1049090, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls h-vpls neighbor 10.255.114.3 vpls-id 100

Mesh-group connections: spokes
Neighbor                  Type  St     Time last up          # Up trans
10.255.114.4 (vpls-id 200)  rmt   Up     Apr 11 23:39:25 2013           1
Remote PE: 10.255.114.4, Negotiated control-word: No
Incoming label: 262148, Outgoing label: 304224
Negotiated PW status TLV: Yes
Local PW status code: 0x00000000, Neighbor PW status code: 0x00000000
Local interface: lsi.1049091, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls h-vpls neighbor 10.255.114.4 vpls-id 200
10.255.114.4 (vpls-id 201)  rmt   Up     Apr 11 23:39:25 2013           1
Remote PE: 10.255.114.4, Negotiated control-word: No
show vpls connections extensive (Static VPLS Neighbors)

```
user@host> show vpls connections extensive instance red

Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <= -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unn connection status      IL -- no incoming label
MM -- MTU mismatch                MI -- Mesh-Group ID not available
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy
RS -- remote site standby        SN -- Static Neighbor

Legend for interface status
Up -- operational
Dn -- down

Instance: static
VPLS-id: 1
Number of local interfaces: 1
Number of local interfaces up: 1
ge-0/0/5.0
lsi.1049344  Intf - vpls static neighbor 10.255.114.3 vpls-id 1

Neighbor     Type   St     Time last up       # Up trans
10.255.114.3(vpls-id 1)(SN) rmt Up     Mar 4 08:48:41 2010           1
Remote PE: 10.255.114.3, Negotiated control-word: No
Incoming label: 29696, Outgoing label: 29697
Negotiated PW status TLV: No
Local interface: lsi.1049344, Status: Up, Encapsulation: ETHERNET
Description: Intf - vpls static neighbor 10.255.114.3 vpls-id 1

Connection History:
Mar 4 08:48:41 2010  status update timer
Mar 4 08:48:41 2010  PE route changed
Mar 4 08:48:41 2010  Out lbl Update                        29697
Mar 4 08:48:41 2010  In lbl Update                        29696
Mar 4 08:48:41 2010  loc intf up                         lsi.1049344
```

user@PE1> show vpls connections extensive (Multihoming with FEC 129)

Layer-2 VPN connections:

<table>
<thead>
<tr>
<th>Legend for connection status (St)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EI -- encapsulation invalid</td>
</tr>
<tr>
<td>EM -- encapsulation mismatch</td>
</tr>
<tr>
<td>VC-Dn -- Virtual circuit down</td>
</tr>
<tr>
<td>CM -- control-word mismatch</td>
</tr>
<tr>
<td>CN -- circuit not provisioned</td>
</tr>
<tr>
<td>OR -- out of range</td>
</tr>
<tr>
<td>OL -- no outgoing label</td>
</tr>
<tr>
<td>LD -- local site signaled down</td>
</tr>
<tr>
<td>RD -- remote site signaled down</td>
</tr>
<tr>
<td>LN -- local site not designated</td>
</tr>
<tr>
<td>RN -- remote site not designated</td>
</tr>
<tr>
<td>XX -- unknown connection status</td>
</tr>
<tr>
<td>MM -- MTU mismatch</td>
</tr>
<tr>
<td>BK -- Backup connection</td>
</tr>
<tr>
<td>PF -- Profile parse failure</td>
</tr>
<tr>
<td>RS -- remote site standby</td>
</tr>
<tr>
<td>LB -- Local site not best-site</td>
</tr>
<tr>
<td>VM -- VLAN ID mismatch</td>
</tr>
<tr>
<td>NC -- interface encapsulation not CCC/TCC/VPLS</td>
</tr>
<tr>
<td>WE -- interface and instance encaps not same</td>
</tr>
<tr>
<td>NP -- interface hardware not present</td>
</tr>
<tr>
<td>SC -- local and remote site ID collision</td>
</tr>
<tr>
<td>LM -- local site ID not minimum designated</td>
</tr>
<tr>
<td>RM -- remote site ID not minimum designated</td>
</tr>
<tr>
<td>IL -- no incoming label</td>
</tr>
<tr>
<td>MI -- Mesh-Group ID not available</td>
</tr>
<tr>
<td>ST -- Standby connection</td>
</tr>
<tr>
<td>PB -- Profile busy</td>
</tr>
<tr>
<td>SN -- Static Neighbor</td>
</tr>
<tr>
<td>RB -- Remote site not best-site</td>
</tr>
<tr>
<td>IL -- no incoming label</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legend for interface status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up -- operational</td>
</tr>
<tr>
<td>Dn -- down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instance: green</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2vpn-id: 100:100</td>
</tr>
<tr>
<td>Local-id: 192.0.2.2</td>
</tr>
<tr>
<td>Number of local interfaces: 2</td>
</tr>
<tr>
<td>Number of local interfaces up: 2</td>
</tr>
<tr>
<td>ge-0/3/1.0</td>
</tr>
<tr>
<td>ge-0/3/3.0</td>
</tr>
<tr>
<td>lsi.101711873</td>
</tr>
<tr>
<td>Intf - vpls green local-id 192.0.2.2</td>
</tr>
<tr>
<td>remote-id</td>
</tr>
<tr>
<td>192.0.2.4 neighbor 192.0.2.4</td>
</tr>
<tr>
<td>Remote-id</td>
</tr>
<tr>
<td>Type  St  Time last up  # Up trans</td>
</tr>
<tr>
<td>192.0.2.4</td>
</tr>
<tr>
<td>rmt  Up  Jan 31 13:49:52 2012  1</td>
</tr>
<tr>
<td>Remote PE: 192.0.2.4, Negotiated control-word: No</td>
</tr>
<tr>
<td>Incoming label: 262146, Outgoing label: 262146</td>
</tr>
<tr>
<td>Local interface: lsi.101711873, Status: Up, Encapsulation: ETHERNET</td>
</tr>
<tr>
<td>Description: Intf - vpls green local-id 192.0.2.2 remote-id 192.0.2.4</td>
</tr>
<tr>
<td>neighbor 192.0.2.4</td>
</tr>
<tr>
<td>Connection History:</td>
</tr>
<tr>
<td>Jan 31 13:49:52 2012 status update timer</td>
</tr>
<tr>
<td>Jan 31 13:49:52 2012 PE route changed</td>
</tr>
<tr>
<td>Jan 31 13:49:52 2012 Out lbl Update</td>
</tr>
<tr>
<td>Jan 31 13:49:52 2012 In lbl Update</td>
</tr>
<tr>
<td>Jan 31 13:49:52 2012 loc intf up</td>
</tr>
<tr>
<td>lsi.101711873</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multi-home:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local-site</td>
</tr>
<tr>
<td>Id  Pref  State</td>
</tr>
<tr>
<td>test         1  100  Up</td>
</tr>
<tr>
<td>Number of interfaces: 1</td>
</tr>
<tr>
<td>Number of interfaces up: 1</td>
</tr>
<tr>
<td>ge-0/3/1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Received multi-homing advertisements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote-PE  Pref  flag  Description</td>
</tr>
<tr>
<td>192.0.2.4  100  0x0</td>
</tr>
</tbody>
</table>
show vpls flood event-queue

**Syntax**
```plaintext
show vpls flood event-queue
```

**Release Information**
Command introduced in Junos OS Release 8.0.

**Description**
Display the pending events in the VPLS flood queue.

**Options**
This command has no options.

**Required Privilege Level**
`view`

**List of Sample Output**
`show vpls flood event-queue` on page 2640

**Output Fields**
Table 218 on page 2639 lists the output fields for the `show vpls flood event-queue` command. Output fields are listed in the approximate order in which they appear.

*Table 218: show vpls flood event-queue Output Fields*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Pending Event</td>
<td>Provides information on the current event in the VPLS flood event queue.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Owner Name</td>
<td>Name of the interface associated with the flood event.</td>
</tr>
<tr>
<td>Pending Op</td>
<td>Pending operation for the event.</td>
</tr>
<tr>
<td>Last Error</td>
<td>Name of the last error encountered.</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of attempts made to update the event queue.</td>
</tr>
<tr>
<td>Pending Event List</td>
<td>List of the events awaiting processing.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Pending Op</td>
<td>Pending operation for the event.</td>
</tr>
<tr>
<td>Event Identifier</td>
<td>Name of the interface associated with the flood event.</td>
</tr>
</tbody>
</table>
### Sample Output

```bash
user@host> show vpls flood event-queue
```

#### Current Pending Event

- **Name:** Flood Nexthop
- **Owner Name:** ge-4/3/0.0
- **Pending Op:** ADD
- **Last Error:** ENOMEM
- **Number of Retries:** 3

#### Pending Event List:

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Pending Op</th>
<th>Event Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood Nexthop</td>
<td>ADD</td>
<td>ge-4/3/0.0</td>
</tr>
<tr>
<td>Flood Route</td>
<td>ADD</td>
<td>ge-4/3/0.0</td>
</tr>
</tbody>
</table>
show vpls flood instance

Syntax

show vpls flood instance
  <brief | detail | extensive>
  <instance-name>
  <logical-system logical-system-name>

Release Information

Command introduced in Junos OS Release 8.0.

Description

Display VPLS information related to the flood process.

Options

none—Display VPLS information related to the flood process for all routing instances.

brief | detail | extensive—(Optional) Display the specified level of output.

instance-name—(Optional) Display VPLS information related to the flood process for the specified routing instance.

logical-system logical-system-name—(Optional) Display VPLS information related to the flood process for the specified logical system.

Required Privilege

view

List of Sample Output

show vpls flood instance on page 2642
show vpls flood instance logical-system-name on page 2642
show vpls flood instance detail on page 2642

Output Fields

Table 219 on page 2641 lists the output fields for the show vpls flood instance command. Output fields are listed in the approximate order in which they appear.

Table 219: show vpls flood instance Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical system</td>
<td>Name of the logical system.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the VPLS routing instance.</td>
</tr>
<tr>
<td>CEs</td>
<td>Number of CE routers connected to the VPLS instance.</td>
</tr>
<tr>
<td>VEs</td>
<td>Number of VE routers connected to the VPLS instance.</td>
</tr>
<tr>
<td>Flood routes</td>
<td>List of all flood routes associated with the VPLS instance.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Prefix for the route.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of route.</td>
</tr>
</tbody>
</table>
### Table 219: `show vpls flood instance` Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>VPLS routing instance or interface associated with the route.</td>
</tr>
<tr>
<td>Nhtype</td>
<td>Next-hop type. For example, <code>flood</code> for a flood route.</td>
</tr>
<tr>
<td>Nhindex</td>
<td>Next-hop index number for the route.</td>
</tr>
</tbody>
</table>

#### Sample Output

**show vpls flood instance**

```
user@host> show vpls flood instance

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>ALL_CE_FLOOD</td>
<td>green</td>
<td>flood</td>
<td>383</td>
</tr>
<tr>
<td>0x47/16</td>
<td>CE_FLOOD</td>
<td>fe-1/2/1.0</td>
<td>flood</td>
<td>388</td>
</tr>
</tbody>
</table>
```

**show vpls flood instance logical-system-name**

```
user@host:__example_ls1__> show vpls flood instance example_ls1

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>ALL_CE_FLOOD</td>
<td>green</td>
<td>flood</td>
<td>383</td>
</tr>
<tr>
<td>0x47/16</td>
<td>CE_FLOOD</td>
<td>fe-1/2/1.0</td>
<td>flood</td>
<td>388</td>
</tr>
</tbody>
</table>
```

**show vpls flood instance detail**

```
user@host:__example_ls1__> show vpls flood instance detail

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Type</th>
<th>Owner</th>
<th>NhType</th>
<th>NhIndex</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>ALL_CE_FLOOD</td>
<td>green</td>
<td>flood</td>
<td>383</td>
</tr>
<tr>
<td>0x47/16</td>
<td>CE_FLOOD</td>
<td>fe-1/2/1.0</td>
<td>flood</td>
<td>388</td>
</tr>
</tbody>
</table>
**show vpls flood route**

**Syntax**

```
show vpls flood route
(all-ce-flood instance-name instance-name <logical-system-name logical-system-name>
| ce-flood interface interface-name)
```

**Release Information**

Command introduced in Junos OS Release 8.0.

**Description**

Display VPLS route information related to the flood process for either the specified routing instance or the specified interface.

**Options**

- `all-ce-flood`—Display the flood next-hop route for all customer edge routers for traffic coming from the core of the network.
- `ce-flood interface interface-name`—Display the flood next-hop route for traffic coming from the specified customer edge interface.
- `instance-name instance-name`—Display the flood routes for the specified instance.
- `logical-system-name logical-system-name`—(Optional) Specify the logical system whose flood routes you want to display. You can only specify the default logical system name for VPLS. The default logical system name is `__example_ls1__` (the name must be entered in the command with the underscore characters).

**Required Privilege Level**

`view`

**List of Sample Output**

- `show vpls flood route all-ce-flood on page 2644`
- `show vpls flood route ce-flood on page 2644`

**Output Fields**

Table 220 on page 2643 lists the output for the `show vpls flood route` command. Output fields are listed in the approximate order in which they appear.

**Table 220: show vpls flood route Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood route prefix</td>
<td>Prefix for the flood route.</td>
</tr>
<tr>
<td>Flood route type</td>
<td>Type of flood route (either CE_FLOOD or ALL_CE_FLOOD).</td>
</tr>
<tr>
<td>Flood route owner</td>
<td>VPLS routing instance or interface associated with the flood route.</td>
</tr>
<tr>
<td>Nexthop type</td>
<td>Next-hop type. For example, flood for a flood route.</td>
</tr>
<tr>
<td>Nexthop index</td>
<td>Next-hop index number for the route.</td>
</tr>
</tbody>
</table>
Table 220: show vpls flood route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces flooding to</td>
<td>Interfaces to which VPLS routes are being flooded.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of VPLS router (CE or VE).</td>
</tr>
<tr>
<td>Nh type</td>
<td>Next-hop type.</td>
</tr>
<tr>
<td>Index</td>
<td>Index number for the flood route.</td>
</tr>
</tbody>
</table>

Sample Output

show vpls flood route all-ce-flood

user@host:__example_ls1__> show vpls flood route all-ce-flood logical-system-name __example_ls1__ instance-name green

Flood route prefix: default
Flood route type: ALL_CE_FLOOD
Flood route owner: green
Nexthop type: flood
Nexthop index: 383

Interfaces Flooding to:
Name    Type    NhType    Index
fe-1/2/1.0  CE       -       -

show vpls flood route ce-flood

user@host:__example_ls1__> show vpls flood route ce-flood interface fe-1/2/1.0

Flood route prefix: 0x47/16
Flood route type: CE_FLOOD
Flood route owner: fe-1/2/1.0
Nexthop type: flood
Nexthop index: 388

Interfaces Flooding to:
Name    Type    NhType    Index
lsi.49152  VE       indr    262142
**show vpls mac-table**

**Syntax**

```
show vpls mac-table
  <age>
  <brief | detail | extensive | summary>
  <bridge-domain bridge-domain-name>
  <instance instance-name>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
  <mac-address>
  <vlan-id vlan-id-number>
```

**Release Information**

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 15.1.

**Description**

Display learned virtual private LAN service (VPLS) media access control (MAC) address information.

**Options**

- **none**—Display all learned VPLS MAC address information.
- **age**—(Optional) Display age of a single mac-address.
- **brief | detail | extensive | summary**—(Optional) Display the specified level of output.
- **bridge-domain bridge-domain-name**—(Optional) Display learned VPLS MAC addresses for the specified bridge domain.
- **instance instance-name**—(Optional) Display learned VPLS MAC addresses for the specified instance.
- **interface interface-name**—(Optional) Display learned VPLS MAC addresses for the specified instance.
- **logical-system (all | logical-system-name)**—(Optional) Display learned VPLS MAC addresses for all logical systems or for the specified logical system.
- **mac-address**—(Optional) Display the specified learned VPLS MAC address information.
- **vlan-id vlan-id-number**—(Optional) Display learned VPLS MAC addresses for the specified VLAN.

**Required Privilege**

view

**List of Sample Output**

- show vpls mac-table on page 2647
- show vpls mac-table (with Layer 2 Services over GRE Interfaces) on page 2647
- show vpls mac-table (with VXLAN enabled) on page 2647
- show vpls mac-table age (for GE interface) on page 2648
- show vpls mac-table age (for AE interface) on page 2648
**show vpls mac-table count on page 2648**  
**show vpls mac-table detail on page 2649**  
**show vpls mac-table extensive on page 2649**

**Output Fields**  
Table 221 on page 2646 describes the output fields for the `show vpls mac-table` command. Output fields are listed in the approximate order in which they appear.

**Table 221: show vpls mac-table Output fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of a single mac-address.</td>
</tr>
<tr>
<td>Routing instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Bridging domain</td>
<td>Name of the bridging domain.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address or addresses learned on a logical interface.</td>
</tr>
<tr>
<td>MAC flags</td>
<td>Status of MAC address learning properties for each interface:</td>
</tr>
<tr>
<td></td>
<td>• S—Static MAC address configured.</td>
</tr>
<tr>
<td></td>
<td>• D—Dynamic MAC address learned.</td>
</tr>
<tr>
<td></td>
<td>• SE—MAC accounting is enabled.</td>
</tr>
<tr>
<td></td>
<td>• NM—Nonconfigured MAC.</td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>MAC count</td>
<td>Number of MAC addresses learned on a specific routing instance or interface.</td>
</tr>
<tr>
<td>Learning interface</td>
<td>Logical interface or logical Label Switched Interface (LSI) the address is learned on.</td>
</tr>
<tr>
<td>Base learning interface</td>
<td>Base learning interface of the MAC address. This field is introduced in Junos OS Release 14.2.</td>
</tr>
<tr>
<td>Learn VLAN ID/VLAN</td>
<td>VLAN ID of the routing instance or bridge domain in which the MAC address was learned.</td>
</tr>
<tr>
<td>VXLAN ID/VXLAN</td>
<td>VXLAN Network Identifier (VNI)</td>
</tr>
<tr>
<td>Layer 2 flags</td>
<td>Debugging flags signifying that the MAC address is present in various lists.</td>
</tr>
<tr>
<td>Epoch</td>
<td>Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Sequence number assigned to this MAC address. Used for debugging.</td>
</tr>
<tr>
<td>Learning mask</td>
<td>Mask of Packet Forwarding Engines where this MAC address was learned. Used for debugging.</td>
</tr>
<tr>
<td>IPC generation</td>
<td>Creation time of the logical interface when this MAC address was learned. Used for debugging.</td>
</tr>
</tbody>
</table>
### Sample Output

**show vpls mac-table**

```bash
user@host> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)

Routing instance: vpls_ldp1
VLAN: 223
<table>
<thead>
<tr>
<th>MAC address</th>
<th>MAC flags</th>
<th>Logical interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:5e:00:53:5d</td>
<td>D</td>
<td>ge-0/2/5.400</td>
</tr>
</tbody>
</table>

MAC flags (S -static MAC, D -dynamic MAC,
SE -Statistics enabled, NM -Non configured MAC)

Routing instance: vpls_red
VLAN: 401
<table>
<thead>
<tr>
<th>MAC address</th>
<th>MAC flags</th>
<th>Logical interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:5e:00:53:12</td>
<td>D</td>
<td>lsi.1051138</td>
</tr>
<tr>
<td>00:00:5e:00:53:f0</td>
<td>D</td>
<td>lsi.1051138</td>
</tr>
</tbody>
</table>
```

**show vpls mac-table (with Layer 2 Services over GRE Interfaces)**

```bash
user@host> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance: vpls_4site:1000
Bridging domain: __vpls_4site:1000__, VLAN: 4094, 4093
VXLAN: Id: 300, Multicast group: 233.252.0.1
<table>
<thead>
<tr>
<th>MAC address</th>
<th>MAC flags</th>
<th>Logical interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:5e:00:53:f4</td>
<td>D,SE</td>
<td>ge-4/2/0.1000</td>
</tr>
<tr>
<td>00:00:5e:00:53:33</td>
<td>D,SE</td>
<td>lsi.1052004</td>
</tr>
<tr>
<td>00:00:5e:00:53:32</td>
<td>D,SE</td>
<td>lsi.1048840</td>
</tr>
<tr>
<td>00:00:5e:00:53:14</td>
<td>D,SE</td>
<td>lsi.1052005</td>
</tr>
<tr>
<td>00:00:5e:00:53:f7</td>
<td>D,SE</td>
<td>gr-1/2/10.10</td>
</tr>
<tr>
<td>00:00:5e:00:53:3f</td>
<td>D,SE</td>
<td>vtep.1052010</td>
</tr>
<tr>
<td>00:00:5e:00:53:3f</td>
<td>D,SE</td>
<td>vtep.1052011</td>
</tr>
</tbody>
</table>
```

**show vpls mac-table (with VXLAN enabled)**

```bash
user@host> show vpls mac-table

MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance: vpls_4site:1000
Bridging domain: __vpls_4site:1000__, VLAN: 4094, 4093
VXLAN: Id: 300, Multicast group: 233.252.0.1
<table>
<thead>
<tr>
<th>MAC address</th>
<th>MAC flags</th>
<th>Logical interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:5e:00:53:f4</td>
<td>D,SE</td>
<td>ge-4/2/0.1000</td>
</tr>
<tr>
<td>00:00:5e:00:53:33</td>
<td>D,SE</td>
<td>lsi.1052004</td>
</tr>
<tr>
<td>00:00:5e:00:53:32</td>
<td>D,SE</td>
<td>lsi.1048840</td>
</tr>
<tr>
<td>00:00:5e:00:53:14</td>
<td>D,SE</td>
<td>lsi.1052005</td>
</tr>
<tr>
<td>00:00:5e:00:53:f7</td>
<td>D,SE</td>
<td>vtep.1052010</td>
</tr>
<tr>
<td>00:00:5e:00:53:3f</td>
<td>D,SE</td>
<td>vtep.1052011</td>
</tr>
</tbody>
</table>
```
show vpls mac-table age (for GE interface)

user@host> show vpls mac-table age 00:00:5e:00:53:1a instance vpls_instance_1

MAC Entry Age information
Current Age: 4 seconds

show vpls mac-table age (for AE interface)

user@host> show vpls mac-table age 000:00:5e:00:53:1a instance vpls_instance_1

MAC Entry Age information
Current Age on FPC1: 102 seconds
Current Age on FPC2: 94 seconds

show vpls mac-table count

user@host> show vpls mac-table count

0 MAC address learned in routing instance __example_private1__

MAC address count per interface within routing instance:

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>lc-0/0/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-0/0/1.0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-0/0/2.0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-2/0/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-0/3/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-2/1/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-9/0/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-11/0/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-2/2/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-9/1/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-11/1/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-2/3/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-9/2/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-11/2/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-11/3/0.32769</td>
<td>0</td>
</tr>
<tr>
<td>lc-9/3/0.32769</td>
<td>0</td>
</tr>
</tbody>
</table>

MAC address count per learn VLAN within routing instance:

<table>
<thead>
<tr>
<th>Learn VLAN ID</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1 MAC address learned in routing instance vpls_ldp1

MAC address count per interface within routing instance:

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsi.1051137</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/2/5.400</td>
<td>1</td>
</tr>
</tbody>
</table>

MAC address count per learn VLAN within routing instance:

<table>
<thead>
<tr>
<th>Learn VLAN ID</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

1 MAC address learned in routing instance vpls_red

MAC address count per interface within routing instance:

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/2/5.300</td>
<td>1</td>
</tr>
</tbody>
</table>
MAC address count per learn VLAN within routing instance:

<table>
<thead>
<tr>
<th>Learn VLAN ID</th>
<th>MAC count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**show vpls mac-table detail**

```
user@host> show vpls mac-table detail

MAC address: 00:00:5e:00:53:5d
Routing instance: vpls_ldp1
    Learning interface: ge-0/2/5.400
    Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
    Epoch: 0          Sequence number: 1
    Learning mask: 0x1                IPC generation: 0

MAC address: 00:00:5e:00:53:5d
Routing instance: vpls_red
    Learning interface: ge-0/2/5.300
    Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
    Epoch: 0          Sequence number: 1
    Learning mask: 0x1                IPC generation: 0
```

**show vpls mac-table extensive**

```
user@host> show vpls mac-table extensive

MAC address: 00:00:5e:00:53:00
Routing instance: vpls_1
    Bridging domain: __vpls_1__, VLAN : NA
    Learning interface: lsi.1049165
    Base learning interface: lsi.1049165
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0          Sequence number: 1
    Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:01
Routing instance: vpls_1
    Bridging domain: __vpls_1__, VLAN : NA
    Learning interface: lsi.1049165
    Base learning interface: lsi.1049165
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0          Sequence number: 1
    Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:02
Routing instance: vpls_1
    Bridging domain: __vpls_1__, VLAN : NA
    Learning interface: lsi.1049165
    Base learning interface: lsi.1049165
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0          Sequence number: 1
    Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:03
Routing instance: vpls_1
    Bridging domain: __vpls_1__, VLAN : NA
    Learning interface: lsi.1049165
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base learning interface</td>
<td>lsi.1049165</td>
</tr>
<tr>
<td>Layer 2 flags</td>
<td>in_hash, in_ifd, in_ifl, in_vlan, in_rtt, kernel, in_ifbd</td>
</tr>
<tr>
<td>Epoch</td>
<td>0</td>
</tr>
<tr>
<td>Sequence number</td>
<td>1</td>
</tr>
<tr>
<td>Learning mask</td>
<td>0x00000001</td>
</tr>
</tbody>
</table>
**show vpls statistics**

**Syntax**

```
show vpls statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**

(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) statistics.

**Options**

- `none`—Display VPLS statistics for all routing instances.
- `instance instance-name`—(Optional) Display VPLS statistics for a specific VPLS routing instance only.
- `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 vpls statistics on page 2652`
- `show vpls statistics instance on page 2653`

**Output Fields**

Table 222 on page 2651 lists the output fields for the `show vpls statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 222: show vpls statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the VPLS instance.</td>
</tr>
<tr>
<td>Local interface</td>
<td>Name of the local VPLS virtual loopback tunnel interface, vt-fpc/pic/port.nnnn, where nnnn is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain.</td>
</tr>
<tr>
<td>Index</td>
<td>Number associated with the next hop.</td>
</tr>
<tr>
<td>Remote provider edge router</td>
<td>Address of the remote provider edge router.</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>Number of multicast packets received.</td>
</tr>
<tr>
<td>Multicast bytes</td>
<td>Number of multicast bytes received.</td>
</tr>
<tr>
<td>Flood packets</td>
<td>Number of VPLS flood packets received.</td>
</tr>
</tbody>
</table>
Table 222: show vpls statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood bytes</td>
<td>Number of VPLS flood bytes received.</td>
</tr>
<tr>
<td>Current MAC count</td>
<td>Number of MAC addresses learned by the interface and the configured maximum limit on the number of MAC addresses that can be learned.</td>
</tr>
</tbody>
</table>

Sample Output

show vpls statistics

user@host> show vpls statistics

VPLS statistics:

Instance: green

Local interface: fe-2/2/1.0, Index: 69
  Multicast packets: 1
  Multicast bytes : 60
  Flooded packets : 18
  Flooded bytes : 2556
  Current MAC count: 1

Local interface: lt-0/3/0.2, Index: 72
  Multicast packets: 3
  Multicast bytes : 153
  Flooded packets : 1
  Flooded bytes : 51
  Current MAC count: 1

Local interface: lsi.32769, Index: 75
  Current MAC count: 0

Local interface: lsi.32771, Index: 77
  Remote PE: 10.255.14.222
  Current MAC count: 2

Instance: red

Local interface: vt-0/3/0.32768, Index: 74
  Multicast packets: 0
  Multicast bytes : 0
  Flooded packets : 0
  Flooded bytes : 0
  Current MAC count: 0

Local interface: vt-0/3/0.32770, Index: 76
  Multicast packets: 0
  Multicast bytes : 0
  Flooded packets : 0
  Flooded bytes : 0
  Current MAC count: 0
show vpls statistics instance

user@host> show vpls statistics instance red

Layer-2 VPN Statistics:
Instance: red

Local interface: vt-3/2/0.32768, Index: 73
Remote provider edge router: 10.255.17.35
Multicast packets: 0
Multicast bytes: 0
Flood packets: 0
Flood bytes: 0
Current MAC count: 1 (Limit 20)